Die mittelständische Wirtschaft im Visier – Bedrohung durch Wirtschaftsspionage und Konkurrenzausspähung

IHK Industrie- und Handelskammer Erfurt

THÜRINGER LANDESAMT FÜR VERFASSUNGSSCHUTZ

Landeskriminalamt Thüringen

Gemeinsames Symposium des Landeskriminalamtes Thüringen und des Thüringer Landesamtes für Verfassungsschutz am 28.11.2006 in Erfurt

Die Beiträge der Gastreferenten bringen die Auffassung der jeweiligen Verfasser zum Ausdruck

Inhaltsverzeichnis

Begrüßung

Gerald Grusser, Hauptgeschäftsführer der Industrie - und Handelskammer Erfurt

Sehr geehrter Herr Staatssekretär Baldus,
meine sehr geehrten Damen und Herren,

sind Sie sich eigentlich sicher, dass Ihr Unternehmen oder Ihre Mitarbeiter nicht von der Konkurrenz ausspioniert werden?
Ich denke, nur die Wenigsten können diese Frage eindeutig mit **nein** beantworten.

Fest steht, insbesondere der Mittelstand hat das Problem der Wirtschaftsspionage bisher weitestgehend unterschätzt.
Lange Zeit wurde angenommen, dass Konkurrenzausspähung lediglich eine Problematik für Konzerne sei.

Aber in Zeiten wo zunehmend Produkte und Dienstleistungen austauschbar werden, wird das Know-how der Unternehmen immer mehr zum entscheidenden Wettbewerbsvorteil.
Gerade Schlüsseltechnologien - beispielsweise im Maschinenbau, der Fahrzeugtechnik aber auch der Unterhaltungselektronik - waren in der Vergangenheit der Garant dafür, dass Deutschland über Jahre hinweg in vielen Sektoren als Exportweltmeister und oft auch als Marktführer agieren konnte.
Allerdings: Die Konkurrenz schläft nicht.
Der Wettbewerb ist gnadenlos und Erfolge von gestern geraten schnell in Vergessenheit.
Spitzentechnologie und Marktführerschaft müssen permanent neu erkämpft werden und nicht immer wird dabei mit redlichen Mitteln agiert.

Der Transfer von „Wissen“ ist durch die neuen technischen Möglichkeiten unkomplizierter denn je.
Sensible Dateien sind schnell kopiert und mit einem einfachen Mausklick an jeden beliebigen Ort der Welt „transportiert“.
Hinzu kommt: Gerade die aufstrebenden Volkswirtschaften in Asien haben schon traditionell ein ganz anderes Verhältnis zum Schutz des geistigen Eigentums oder der Bedeutung von Patenten.
Die möglichst detailgerechte Kopie des Originals, d.h. die Anfertigung eines Plagiats, wird mehr als Herausforderung und nicht als moralisch verwerflich betrachtet.

Die Folgen für die Unternehmen - aber auch die Volkswirtschaft - sind immens: neue Wettbewerber die mit wesentlich geringeren Kosten agieren bieten quasi ohne Entwicklungsvorlauf vergleichbare Produkte zu deutlich niedrigeren Preisen auf dem Weltmarkt.
Der Verlust von Marktanteilen, der Margenverfall, der Verlust von Arbeitsplätzen und im schlimmsten Fall die Insolvenz des Unternehmens sind die Resultate dieser fatalen Entwicklung.

„Willkommen in der Denkfabrik.“ Mit diesem Slogan wirbt Thüringen als Standort für Investoren.
Zahlreiche High-Tech-Unternehmen haben sich im Freistaat angesiedelt. Das Thema der Wirtschaftsspionage sollte deshalb von keinem Unternehmen unterschätzt werden.

Dabei sind es weniger „James Bond-Praktiken“ - oft sind es die ganz banalen Dinge, die es leicht machen, an die Daten Ihres Unternehmens zu kommen.

Der Einsatz der neuen elektronischen Medien eröffnet vielfältige Möglichkeiten: mit einfachen Mitteln ist ein Datendiebstahl bereits möglich, wenn Mitarbeiter oder auch Geschäftsführer die vorhandene Sicherheitstechnologie nicht richtig einsetzen oder sie sogar für überflüssig erachten.
Der potenzielle Angreifer braucht nicht viel Know-how, um eine solche Sicherheitslücke auszunutzen: ein Notebook, die Adresse des Managers und die richtige Software reichen dabei oft schon aus.
Meine Damen und Herren,
stellen Sie sich deshalb rechtzeitig dieser Problematik.
Nutzen Sie das Know-how unserer heutigen Referenten, diskutieren Sie mit den Experten und schließen Sie mögliche Sicherheitslücken auch in Ihrem Betrieb!

Ich freue mich, dass wir mit dem Landeskriminalamt Thüringen und dem Thüringer Landesamt für Verfassungsschutz wichtige Kooperationspartner für diese Veranstaltung gewinnen konnten, bedanke mich beim Staatssekretär im Thüringer Innenministerium, Herrn Stefan Baldus für seine persönliche Mitwirkung und den Präsidenten Helmut Huber und Thomas Sippel für die fachliche Vorbereitung und Begleitung des Symposiums.

Eröffnung

Stefan Baldus, Staatssekretär im Thüringer Innenministerium

Sehr geehrter Herr Grusser,
sehr geehrter Herr Huber,
sehr geehrter Herr Sippel,
meine sehr verehrten Damen und Herren,

„Die wichtigen Schlachten finden tatsächlich in der Wirtschaft statt. Die Auseinandersetzungen im politischen Sektor sind hingegen uninteressant, mittelmäßig und vergleichsweise unbedeutend".

Auch wenn man sich diesem Zitat von Jean-Jacques Servan-Schreiber, französischer Publizist und Unternehmer, in Bezug auf die Bewertung des Politischen nicht vollinhaltlich anschließen mag, so verdeutlicht es doch treffend den Stellenwert, den eine gesunde Volkswirtschaft für den weltpolitischen Geltungswert eines Landes besitzt. Längst hat sich im Rahmen der wirtschaftlichen Globalisierung der kompromisslose Wettbewerb um wissenschaftlich-geistige Ressourcen und technologische Innovationspotentiale zu einer Auseinandersetzung entwickelt, deren Ausgang die Zukunftsfähigkeit einer Nation und somit ihren internationalen Stellenwert entscheidend mitbestimmen wird.

Zwar gelang es der Bundesrepublik Deutschland nach 1949, trotz gravierender soziostruktureller Umwälzungen und unter oft genug schwierigen weltpolitischen Rahmenbedingungen im Schatten des Ost-West-Konfliktes eine ökonomische Spitzenposition in den Reihen der westlichen Industrienationen zu erringen. Die Gründe hierfür lagen zuvorderst in der Erfolgsträchtigkeit des von Ludwig Erhart begründeten Konzeptes der sozialen Marktwirtschaft sowie in der maßgeblich von Konrad Adenauer initiierten Verankerung der Bundesrepublik in einem einheitlichen europäischen Wirtschaftsraum, die von allen folgenden Bundesregierungen weiter geführt wurde und deutschen Produkten einen hoch aufnahmefähigen Absatzmarkt quasi „vor der Haustür" verschaffte.

Doch die Erfolgsstory währte nicht ewig: mit den weltpolitischen Veränderungen 1989, die eine historische Zäsur epochalen Ausmaßes markierten, änderten sich die Grundaxiome der politischen Interaktion von Staaten und Bündnissen fundamental.

Bemaß sich bislang die machtpolitische Geltungskraft eines Staates bzw. eines Bündnisses primär aus der Schlagkraft von Streitkräften, und erst in zweiter Linie aus wirtschaftlicher Potenz, so trat nun eine sich mit atemberaubender Geschwindigkeit vollziehende Bedeutungserosion dieser „klassischen" Instrumente staatlicher Machtprojektion ein.

Dieser Bedeutungsschwund, der sich aus dem Ende der historischen Blockkonfrontation ergab, führte in Verbindung mit einer grund-legenden Neuordnung der internationalen Verhältnisse (Stichwort: „New World Order") sowie dem Erstarken neuer Akteure auf der weltpolitischen Bühne zu einer stärkeren Fokussierung auf ökonomische Potentiale und wirtschaftspolitisches Durchsetzungsvermögen als Maßstäbe für die Bedeutung eines Landes im internationalen Konkurrenzkampf.

Naturgemäß war auch die Bundesrepublik Deutschland als stärkste Wirtschaftsmacht der Europäischen Union von dieser Dynamik betroffen.

So musste sich auch die deutsche Wirtschaft in der vergangenen Dekade auf die neuen Herausforderungen einstellen und in oftmals schmerzhaften Anpassungsprozessen die „richtige“ Antwort auf die drängenden Probleme der ökonomischen Globalisierung finden.

Zu Beginn des 21. Jahrhunderts stehen auch die Thüringer Unternehmen in einem globalen Wettbewerb. Für wirtschaftlichen Erfolg auf den internationalen Märkten sind Innovationsfähigkeit, Flexibilität, genaue Information und schnelle Kommunikation unabdingbar. Das frühzeitige Erkennen von Chancen und Risiken bringt ebenso wie die Entwicklung neuer Ideen und deren schnelle Umsetzung in ein Produkt oder in eine Strategie entscheidende Vorteile gegenüber vorhandenen und potentiellen Konkurrenten. Für Wettbewerber ist das Know-how der erfolgreichen Unternehmen des Wirtschaftsstandorts Deutschland eine wertvolle Quelle – besonders, aber keinesfalls ausschließlich, für solche aus den aufstrebenden Wirtschaftsnationen Asiens.

Die unberechtigte Beschaffung von Informationen, der Diebstahl von Ideen, von Betriebs- und Geschäftsgeheimnissen, von ebenso mühsamer wie wertvoller Forschungs- und Entwicklungsarbeit, der Missbrauch von Patenten, Marken und Urheberrechten sind in hohem Maße geeignet, Unternehmen schwer und nachhaltig zu schädigen. Das Unrechtsbewusstsein ist dabei in ausländischen Unternehmen vielfach anders bis gar nicht ausgeprägt.

Auch muss man sich bewusst sein: Nach dem Ende des Kalten Krieges hat sich Schwerpunkt der Tätigkeit von Agenten fremder Nachrichtendienste erheblich verlagert, vor allem in Richtung des - wenn ich es einmal so nennen darf – „lukrativen Geschäftes“ der Wirtschaftsspionage.

Die Wirtschaftsspionage – also die Informationsbeschaffung durch fremde Nachrichtendienste - und die Ausspähung von Unternehmen durch andere, konkurrierende Unternehmen der Privatwirtschaft stellen eine zunehmende Bedrohung für deutsche und damit auch thüringische Unternehmen dar.

Dieser Bereich der Wirtschaftskriminalität steht deshalb im Mittelpunkt des heutigen Symposiums, zu dem ich Sie sehr herzlich begrüßen darf.

Meine Damen und Herren,

die Wirtschaftsprüfungs- und Beratungsgesellschaft KMPG kommt in ihrer aktuellen Studie zum Thema Wirtschaftskriminalität vom Juli dieses Jahres zu besorgniserregenden Ergebnissen. Wirtschaftskriminalität umfasst in diesem Zusammenhang eine Vielzahl von Handlungsweisen - angefangen vom Lagerdiebstahl über Untreue bis hin zu Bilanzfälschungen - und eben auch die Verletzung von Betriebs- und Geschäftsgeheimnissen.

Die Unternehmensbefragung ergab, dass in den vergangenen drei Jahren 55 Prozent der großen Unternehmen von wirtschaftskriminellen Handlungen betroffen waren. Bei den mittleren Unternehmen sind es 31, bei den kleineren immerhin 19 Prozent, also fast jedes fünfte Unternehmen.

Auch wenn nach diesen eigenen Angaben vor allem große Unternehmen betroffen sind, ist Wirtschaftskriminalität auch für kleine und mittlere Unternehmen eine ernst zunehmende Bedrohung.

Denn die Studie geht davon aus, dass der Zusammenhang zwischen Unternehmensgröße und der Betroffenheit von wirtschaftskriminellen Handlungen wohl auch daraus resultiert,

dass in größeren Unternehmen aufgrund besserer Organisations- und Kontrollmechanismen mehr wirtschaftskriminelle Straftaten aufgedeckt werden.
Vor diesem Hintergrund sind auch die Angaben der polizeilichen Kriminalstatistik zu wirtschaftskriminellen Straftaten zu bewerten.

Laut Bundeskriminalamt macht die Wirtschaftskriminalität nur 1,4 % der von der Polizei bundesweit erfassten Straftaten aus. Gleichwohl verursachen diese 1,4 % die Hälfte des Gesamtschadens aller Straftaten, die mit einer Schadenssumme erfasst werden können. Dabei spiegeln die Zahlen der polizeilichen Statistik natürlich nur die polizeilich erfassten Fälle wider, nicht beispielsweise die von Zoll- und Finanzämtern verfolgten Straftaten und erst recht nicht die gar nicht erkannten oder nicht angezeigten Fälle.

Das tatsächliche Aufkommen von Straftaten aus dem Bereich der Wirtschaftskriminalität und der entstehende Schaden dürften noch um ein Vielfaches höher liegen. Nach Einschätzung der für die KPMG-Studie befragten Unternehmen kommen auf jeden entdeckten Fall von Wirtschaftskriminalität fünf unentdeckte.

Die zu vermutende hohe Dunkelziffer liegt zum einen daran, dass sich viele Unternehmen scheuen, sich mit durchaus erkannten Sicherheitsproblemen an die staatlichen Behörden zu wenden oder gar über Sicherheitsprobleme öffentlich zu sprechen. Befürchtet wird ein Vertrauens- und Reputationsverlust bei Kunden, Lieferanten, Kreditinstituten, der nachhaltige Schädigungen des Unternehmens zur Folge haben kann. Außerdem wurden 59 Prozent der erkannten kriminellen Handlungen nur durch Zufall aufgedeckt.

All dies ist äußerst alarmierend und sollte auch für Thüringer Unternehmer Anlass sein, die Problematik ernst zu nehmen.

Meine Damen und Herren,

um bei der Bekämpfung von Wirtschaftskriminalität Erfolge zu erzielen, müssen Privatwirtschaft und Sicherheitsbehörden eng zusammenarbeiten. Frühzeitige Beratung und Prävention sind dabei die wichtigsten Mittel.

Die KPMG hat nämlich auch ermittelt, dass mehr als die Hälfte der befragten Unternehmen ihre Kenntnisse über typische wirtschaftskriminelle Vorgehensweisen als schlecht oder eher schlecht bewerten.

Darüber hinaus glauben 58 Prozent der Befragten, dass bei höherer Sensibilität ihrer Mitarbeiter die Vorkommnisse in ihren Unternehmen hätten vermieden werden können.

Geschärftes Problembewusstsein und die Sensibilisierung von Unternehmensführung und Mitarbeitern für die Gefahren der Wirtschaftsspionage und Konkurrenzausspähung sind der erste Schritt auf dem Weg zu wirkungsvollen Präventionsmaßnahmen. Dem dient auch das heutige gemeinsame Symposium der Industrie- und Handelskammer Erfurt, des Thüringer Landeskriminalamtes und des Landesamtes für Verfassungsschutz.

Sie können sich als Unternehmen durchaus mit verschiedensten Sicherheitsvorkehrungen gegen Wirtschaftsspionage und Konkurrenzausspähung schützen. Dies kann beginnen bei einer Verbesserung der Sicherheit der Informationstechnologie, bei der Dokumentensicherung, beim Zugangsmanagement, Kontrollsystemen und so weiter. Die Sicherheitsbehörden können Ihnen dazu wertvolle Ratschläge geben.

Ich wünsche Ihnen deshalb eine interessante Tagung mit ergiebigen Beiträgen, die Sie sich für ihre Unternehmen nutzbar machen können. Gleichzeitig möchte ich Sie ermutigen, sich

auch nach dem Symposium nicht zu scheuen, mit den Thüringer Sicherheitsbehörden in Kontakt zu bleiben.

Nicht nur, wenn Sie konkrete Hinweise oder Befürchtungen haben, sondern auch, wenn Sie sich über präventive Maßnahmen beraten lassen wollen und frühzeitig Unterstützung in Anspruch nehmen wollen. Von einer intensiven Zusammenarbeit zwischen Wirtschaft und Sicherheitsbehörden können Sie nur profitieren.

Wirtschaftsspionage und Proliferation –
verdeckte Bedrohung für technologieorientierte Unternehmen

Martin Kaufmann, Thüringer Landesamt für Verfassungsschutz

Meine sehr verehrten Damen und Herren,

die weltweiten politischen Veränderungen der vergangenen 16 Jahre, deren Ausgangs- und zugleich Kulminationspunkt das Ende der Ost-West-Konfrontation markiert, führte zum Wegfall einer ganzen Reihe von äußeren Sicherheitsrisiken für die Bundesrepublik. Ihre Abwehr bestimmte maßgeblich die Arbeit der bundesdeutschen Sicherheitsbehörden über vier Jahrzehnte hinweg. Trotz der vermeintlichen Entspannung der Sicherheitslage sahen sich diejenigen, die zu Beginn der 90er Jahre das Zeitalter immerwährender Freundschaft und grenzenlosen Vertrauens zwischen den Völkern gekommen wähnten, spätestens ab Mitte der 90er Jahre u.a. durch die teils turbulenten, nicht immer friedlichen Entwicklungen auf dem Gebiet der ehemaligen Sowjetunion, den Aufstieg Chinas zur „Weltmacht in Wartestellung“ und das Erstarken neuer, oft zweifelhafter staatlicher Akteure auf der weltpolitischen Bühne in ihren optimistischen Prognosen widerlegt. Viele sicherheitspolitische Herausforderungen überlebten diese Zeit des globalen Umbruchs und beschäftigen nunmehr erneut die Sicherheitsbehörden unseres Landes. Zu diesen dauerhaft virulenten Gefahren für die innere Sicherheit der Bundesrepublik zählt auch die Spionage durch fremde Nachrichtendienste, ein Problem, das sich trotz Wegfall der Aufklärung durch die DDR-„Staatssicherheit“ weder hinsichtlich seiner Qualität noch seiner Quantität substantiell entschärft hat. Im Gegenteil: Die Zahl der Staaten, die mit unterschiedlichen Zielsetzungen Ausforschung gegen die Bundesrepublik Deutschland betreiben, ist in den vergangenen 10 Jahren in dem Maße gestiegen, in dem auch die Liberalisierung der Weltmärkte den zwischenstaatlichen Wettbewerb um zukunftsträchtiges Know-how und Wissenspotentiale erhitzt hat. Folgerichtig bezeichnet das Bundesamt für Verfassungsschutz – in Deutschland zentral verantwortlich für alle Belange der Spionageabwehr – in seinem Bericht für das Jahr 2005 die Bundesrepublik als „[...] *weiterhin* [..] *wichtiges Aufklärungsziel für die Nachrichtendienste fremder Staaten*“ und ergänzt, dass sich „*das Bedrohungsszenario im Aufgabenbereich der Spionageabwehr* [...] *im Jahr 2005 nicht verändert* [hat]“. Offensichtlich ist die Bundesrepublik Deutschland wegen ihrer zentralen Lage in Europa, ihrer Wirtschaftskraft und ihrem infolge der Vereinigung noch gewachsenen politischen Gewicht nach wie vor ein bevorzugtes Ausspähungsziel der Nachrichtendienste fremder Staaten. Auch wenn Spionagefälle nur sporadisch ans Licht der Öffentlichkeit gelangen und es selten zur Verurteilung überführter Agenten kommt, gilt es also, dem Anschein trügerischer Sicherheit zu wehren und sich offensiv mit den Herausforderungen durch die entsprechenden Begehrlichkeiten fremder Staaten auseinander zu setzen. Diese richten sich nicht zuletzt auf das Feld der Wirtschaft, da sich das internationale politische Gewicht eines Landes durch die Gesetzmäßigkeiten der Globalisierung zwischenzeitlich nicht mehr ausschließlich aus seinem militärischen, sondern auch aus seinem ökonomischen Potential bemisst. Aus diesem Grunde widme ich den ersten Teil meiner Darlegungen einer genaueren Betrachtung der Wirtschaftsspionage, d.h. einem Spionagefeld, das nach dem Ende des Ost-West-Konflikt angesichts eines fortgeschrittenen weltweiten ökonomischen Verdrängungswettbewerbes zunehmend wichtiger geworden ist.

Ein weiteres Problem, das angesichts der angespannten internationalen politischen Lage weiterhin die besondere Aufmerksamkeit der Sicherheitsbehörden fordert, ist das der Proliferation, also des (illegalen) Handels mit A-,B- oder C-Waffen. So versucht eine Reihe von Staaten unter Umgehung nationaler und internationaler Kontrollregimes und

Embargobestimmungen weiterhin, in den Besitz von ABC-waffenfähigen Vorprodukten bzw. relevanten Rüstungsgütern zu gelangen, um auf diese Weise ihre Streitkräfte aufzurüsten und sich im Kampf um internationale Anerkennung und regionale Vormachtstellungen eine günstige Ausgangsposition zu verschaffen. Um diese durchgängig nichtdemokratischen Systeme nicht ungewollt zu stützen, sich gegen Erpressungsversuche diktatorischer Regimes abzusichern und ihre außen- und sicherheitspolitische Handlungsfreiheit zu wahren, hat die Bundesregierung einem Kreis ausgewählter Sicherheitsbehörden – darunter auch der Spionageabwehr des Verfassungsschutzes – den Auftrag erteilt, entsprechende Bestrebungen abzuwehren. Um Sie im Sinne eines ganzheitlichen Bekämpfungsansatzes auch auf diesem Gebiet zu sensibilisieren und dadurch einen Beitrag zur „Prävention durch Information“ zu leisten, wird sich der zweite Abschnitt meines Referates dem Problem der Proliferation zuwenden, also Akteure, Hintergründe, Interessenlagen und Erscheinungsformen beleuchten.

Wirtschaftsspionage

Was ist Wirtschaftsspionage?

In der Öffentlichkeit wird häufig nicht zwischen Wirtschaftsspionage und Konkurrenzausspähung („Industriespionage“) unterschieden. Daher ist zunächst eine Abgrenzung beider Begriffe erforderlich.

Unter Konkurrenzausspähung versteht man die Ausforschung, die ein (konkurrierendes) Unternehmen gegen ein anderes betreibt. Sie ist rein privatwirtschaftlicher Natur und eröffnet somit nicht den Aufgabenbereich der Verfassungsschutzbehörden. Nichtsdestotrotz kann eine Strafbarkeit vorliegen, wenn z.B. Urheber- oder Patentrechte der ausgespähten Firma verletzt oder Betriebsgeheimnisse auf illegalem Wege, beispielsweise durch Diebstahl, erlangt werden.

Unter Wirtschaftsspionage versteht man hingegen die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben. Ihre Strafbarkeit ist in den §§ 93-100 StGB niedergelegt. Dieser Bereich nachrichtendienstlicher Tätigkeit ist Aufgabe der Spionageabwehr der Verfassungsschutzbehörden.

Warum Wirtschaftspionage?

Die Motive eines Staates, seine Nachrichtendienste auf die deutsche Wirtschaft anzusetzen, erklären sich in erster Linie aus den Rahmenbedingungen der wirtschaftlichen Globalisierung und den damit verbundenen gravierenden inneren Umwälzungen, denen sich die jeweiligen nationalen Volkswirtschaften ausgesetzt sehen. Die sich seit dem Ende des Ost-West-Konfliktes beschleunigende Entwicklung, zwischenstaatliche Konflikte um Macht und Ressourcen auf neue, wirtschaftliche Schauplätze zu verlagern, hat in der Konsequenz dazu geführt, daß die Wirtschaftskraft eines Staates mittlerweile gleichzusetzen ist mit seiner Bedeutung im weltpolitischen Gefüge; diese Wirtschaftskraft mit allen Mitteln, so auch durch Spionage, zu erhalten bzw. zu stärken, gehört mithin zur Staatsräson vieler Nationen der Erde. Folglich zählt insbesondere in Ländern, in denen Wirtschaft und staatliche Strukturen eng miteinander verflochten sind, aktive Aufklärung im ökonomischen Bereich zum normalen Instrumentarium staatlicher Existenzvorsorge. In diesem Zusammenhang sollte unser Blick jedoch nicht nur Ländern aus dem Kreise der „üblichen Verdächtigen“ , z.B. China, Iran usw., gelten, deren Wirtschaft immer noch weitgehend verstaatlicht ist. Auch Staaten, die zum Zirkel der engsten Freunde und Verbündeten Deutschlands zählen, begreifen ihre Wirtschaft trotz diverser Freihandelsabkommen in erster Linie als nationales Schutzgut, dessen Prosperität es mit allen Mitteln zu wahren bzw. durchzusetzen gilt.

Abgesehen von diesen eher staatspolitisch-abstrakten Motiven, die den Bezugsrahmen für Wirtschaftsspionage gegen die Bundesrepublik markieren, diktiert jedoch auch die drastische Veränderung der globalen Wissens- und Informationskultur die fortdauernden Bestrebungen fremder Staaten, ökonomisch verwertbares Wissen von potentiellen Konkurrenten zu erlangen: in der globalen Informationsgesellschaft, in der wir leben, ist der strategische Wert von Informationen auch im wirtschaftlichen Bereich enorm gestiegen, da auf der Zeitachse der Einführung neuer Produkte durch Spionage erlangte Informations- und Wissensvorsprünge unmittelbare Wettbewerbsvorteile eröffnen. So ermöglichen sie z.B. eine frühzeitige Positionierung am Markt, die „verspätete" Konkurrenten vom Marktgeschehen nahezu ausschließt. Eine auf diesem Wege eroberte beherrschende Marktstellung ist zugleich ein wirtschaftlicher Aktivposten gegen den Verlust von Arbeitsplätzen im eigenen Land, der jeder Regierung innenpolitische Schwierigkeiten bereiten würde. Zudem helfen die auf nachrichtendienstlichem Wege beschafften Informationen, im Bereich der Produktentwicklung Zeit und, angesichts des harten internationalen Wettbewerbes mindestens ebenso wichtig, hohe Kosten für eigene Forschungsvorhaben einzusparen, da keine Entwicklungsabteilungen unterhalten und mit teuren Fachleuten besetzt werden müssen.

Welche Wirtschaftsbereiche sind besonders gefährdet?

Worin bestehen die operativen Ziele fremder Nachrichtendienste?

Wissenschaft und Technologie sind bevorzugte Ziele der Wirtschaftsspionage. Das besondere Interesse fremder Dienste richtet sich in diesem Zusammenhang auf Unternehmen und Forschungseinrichtungen der Rüstungs- und Materialtechnik, der Computertechnologie, Bio- und Medizintechnik, der Mikro-, Informations- und Kommunikationstechnik, der Luftfahrt- und Verkehrstechnik sowie der Energie- und Umwelttechnologie.

Die operativen Schwerpunkte fremder Nachrichtendienste bei der Ausspähung der deutschen Wirtschaft variieren je nach dem ökonomischen Hintergrund des beteiligten Staates; im allgemeinen sind sie indes deutlich subtiler definiert als der klassische „Blaupausendiebstahl" aus den herkömmlichen Agententhrillern dies nahe legt.

So sind die Begehrlichkeiten hochentwickelter Länder eher im wirtschaftsstrategischen Bereich angesiedelt, sie richten sich auf die wirtschaftliche Infrastruktur der Bundesrepublik im Ganzen, auf energiewirtschaftliche Informationen sowie auf Unternehmens-, Wettbewerbs- und Marktstrategien. Aber auch Preisgestaltung und Konditionen (insbesondere bei großen Ausschreibungen) sowie Zusammenschlüsse und Absprachen von Unternehmen sind in diesem Zusammenhang von besonderem Interesse, genauso wie Informationen über firmeninterne Entscheidungsprozesse sowie über leitende Angestellte in Führungsfunktionen bzw. die mit der Forschungs- und Entwicklungstätigkeit im Unternehmen befassten Mitarbeiter.

Technologisch weniger entwickelte Staaten (Schwellenländer) hingegen versuchen vor allem, sich technisches Know-how zu beschaffen, um Kosten für eigene Entwicklungen oder Lizenzgebühren zu sparen. Darüber hinaus sind sie stark an Informationen über spezielle Fertigungstechniken interessiert, um auf dem Markt mit kostengünstigeren Nachbauten konkurrenzfähig zu sein. Insgesamt gilt für diesen Bereich der eher produktgebundenen Wirtschaftsspionage, dass die entsprechenden Ausforschungsbemühungen auf alle Entwicklungsstufen zielen: von der Forschung und Entwicklung bis zur Fertigung und Vermarktung neuer Produkte.

Nachrichtendienste als Träger der Wirtschaftsspionage

Auslandsaufklärung wird vermutlich von jedem Staat der Erde betrieben, um ein umfassendes Lagebild zur Vorbereitung politischer Entscheidungen zu erlangen. Einige Nachrichtendienste haben in diesem Rahmen auch die Aufgabe, die Wirtschaft ihres Landes unmittelbar zu unterstützen, indem sie für Unternehmen ihres Heimatlandes Informationen beschaffen, die diesen sonst nicht oder nur mit erheblichem Aufwand zugänglich wären. In einigen Ländern sind neben den Auslandsaufklärungsdiensten auch die Inlandsdienste – also die klassischen Abwehrdienste – mit dieser Aufgabe betraut.

Gemessen am Umfang und der Qualität ihrer Aufklärung zählen sicherlich die verschiedenen Dienste Russlands bzw. weiterer GUS-Republiken sowie Chinas zu den Hauptakteuren auf dem Gebiet der gegen die Bundesrepublik gerichteten Wirtschaftsspionage. Insbesondere für Russland gilt der Grundsatz, dass der Wunsch nach politischer Annäherung und wirtschaftlicher Zusammenarbeit nicht gleichzusetzen ist mit dem Verzicht auf nachrichtendienstliche Informationsbeschaffung beim vermeintlichen „Partner", zumal die russischen Dienste ohnehin per Gesetz verpflichtet sind, die Wirtschaft ihres Landes zu „unterstützen".

Aber auch China sieht offensichtlich keinen Widerspruch in seinem Wunsch nach politischer und wirtschaftlicher Zusammenarbeit mit Deutschland und seinem Bestreben, zum Wohle der eigenen Wirtschaft unser Land mit illegalen Mitteln und Methoden auszuforschen. So ist China bei der Realisierung seines ehrgeizigen Planes, noch vor dem Jahr 2020 weltweit führende Wirtschaftsmacht zu sein, in besonderer Weise auf die Aufklärungsergebnisse seiner insgesamt sechs Nachrichten- und Sicherheitsdienste angewiesen, in deren Reihen auch der mittlerweile wahrscheinlich größte Nachrichtendienst der Welt angesiedelt ist. Es handelt sich hierbei um das chinesische „Ministerium für Staatssicherheit" mit einem geschätzten Personalbestand von mehr als 800.000 Mitarbeitern, dem gleichermaßen Aufklärungskompetenzen nach außen und abwehrende Aufgaben im Innern zugewiesen sind.

Darüber hinaus betreiben jedoch auch die Nachrichtendienste des Nahen und Mittleren Ostens (Iran, Syrien, Nordkorea, Pakistan...) sowie Indiens eine gleichbleibend intensive Aufklärung in und gegen Deutschland. Zwar gilt ihr Hauptaugenmerk zumeist der Beschaffung von ABC-Waffen und ist somit im Bereich der Proliferation anzusiedeln, doch da die Grenzen fließend sind, sind sie teilweise auch auf dem Gebiet der Wirtschaftsspionage tätig.

Mittel und Methoden der Wirtschaftsspionage

Zu den Arbeitsmethoden der Aufklärungsdienste gehören sowohl die sog. „offene Informationsbeschaffung", als auch die konspirative Nachrichtenbeschaffung mit geheimen Mitteln.

Da sich heutzutage Informationen, die früher nur durch Agenten zu erlangen waren, durch den Einsatz neuer Technologien verhältnismäßig leicht und zudem risikoarm erschließen lassen, liegt der Anteil der durch Nachrichtendienste auf offenem Wege zusammengetragenen Erkenntnisse bei etwa 80%. Dies wird auch dadurch begünstigt, dass vieles, was früher als „vertraulich" gehandhabt wurde, mittlerweile aufgrund einer spürbaren Erosion des allgemeinen Sicherheitsbewusstseins in der Industrie publiziert oder in anderer Form öffentlich zugänglich gemacht wird. So zählt zu den Methoden der offenen Informationsbeschaffung eine gezielte Auswertung von Veröffentlichungen z.B. in Dissertationen, Fachzeitschriften, im Internet, in wissenschaftlichen Datenbanken und Produktbeschreibungen genauso wie der Besuch öffentlicher Veranstaltungen, wie: Messen, Kongresse, Symposien usw. Dort erlangen Mitarbeiter der Dienste im Zuge der sog.

„Gesprächsabschöpfung“, also zielgerichteter Gespräche, bei denen der jeweilige Gesprächspartner nicht um die nachrichtendienstliche Anbindung seines Gegenüber weiß, eine Fülle an Erkenntnissen und Insiderwissen.

Darüber hinaus nehmen Personen mit nachrichtendienstlichem Hintergrund in Deutschland an Studiengängen und wissenschaftlichen Forschungsprojekten teil oder arbeiten im Rahmen von Trainee- und Praktikantenprogrammen in deutschen Firmen. Durch das Zusammentragen vieler verschiedener Informationsbruchstücke werden fremde Nachrichtendienste auf diesem Wege in die Lage versetzt, Gesamtbilder ihrer Aufklärungsziele zu erstellen.

Die hierbei festgestellten Wissenslücken versucht man auf konspirativem Wege, also durch den Einsatz geheimer Mittel zur Nachrichtenbeschaffung, zu schließen. Hierzu zählt zunächst der „klassische“ Einsatz von Agenten, die auf verschiedenen Umwegen an die betroffenen Firmen und Forschungseinrichtungen herangespielt werden, z.B. als Mitarbeiter privatwirtschaftlicher Unternehmen ihres Heimatlandes oder als (Wirtschafts-) Journalisten getarnt. Darüber hinaus werden gezielt Mitarbeiter „interessanter“ Firmen zur geheimen Zusammenarbeit angeworben; in Einzelfällen werden auch persönliche Druckmittel, sog. Kompromate, eingesetzt, um eine solche Zusammenarbeit zu forcieren. Auch die breitflächige Überwachung von Telekommunikation bzw. das Eindringen in (geschützte) IT-Systeme via Internet zählt mittlerweile zum gängigen Repertoire der betreffenden Dienste. Etwa 20% des relevanten Erkenntnisaufkommens fremder Nachrichtendienste im wirtschaftlichen Bereich speist sich aus diesen Methoden der geheimen Nachrichtenbeschaffung.

Falldarstellung

Meine Damen und Herren, nun, da ich Sie sozusagen mit dem „theoretischen Rüstzeug“ zum Thema Wirtschaftspionage versehen habe, möchte ich anhand einiger abstrahierter Fälle aus dem Arbeitsalltag der Verfassungsschutzbehörden Ihren Blick dafür schärfen, wie diese Form von Spionage in der Praxis funktioniert.

Vertrauenswürdiger Insider/1

Bei einem deutschen Rüstungszulieferer war eine chinesische Mitarbeiterin auffällig geworden, die sich im Laufe ihrer erst kurzen Betriebszugehörigkeit Firmendaten im Umfang von über 150 CDs verschafft hatte. Die CDs wurden bei einer Hausdurchsuchung in ihrer Wohnung aufgefunden. Auffällig war ferner, dass sich die Chinesin kurz vor diesem Ereignis bei einem weiteren baden-württembergischen Rüstungsunternehmen beworben hatte und dort eingestellt werden sollte. Eine nachrichtendienstliche oder zumindest staatliche Steuerung der Chinesin ist angesichts der Zielobjekte zu vermuten. Der Fall ist Gegenstand eines aktuellen Ermittlungsverfahrens.

Vertrauenswürdiger Insider/2

Ein nachrichtendienstlicher Mitarbeiter der chinesischen Botschaft kontaktierte einen chinesischen Wissenschaftler, der bei einem bayerischen Rüstungszulieferer tätig war. Auf Anforderung lieferte der chinesische Wissenschaftler Informationen über weitere bei der Firma beschäftigte chinesische bzw. chinesischstämmige Mitarbeiter. Zu diesen zählte auch ein chinesischer Wissenschaftler, der in hervorgehobener Funktion in der Entwicklungsabteilung des Unternehmens beschäftigt und dort für entscheidende technische Neuentwicklungen verantwortlich war. Dieser Wissenschaftler wurde daraufhin zu einem Symposium nach China eingeladen. Er nahm daran teil, ohne seinen Arbeitgeber darüber zu informieren. Auch bei einer Sicherheitsüberprüfung verschwieg er seine Reise nach China und die Teilnahme an dem Symposium.

Dieser Fall untermauert die Vermutung der Verfassungsschutzbehörden, dass chinesische Nachrichtendienste Aufenthalte in China u.U. gezielt zur Abschöpfung der chinesischen Wissenschaftler und Ingenieure aus Gastländern nutzen.

ND-Aktivität unter privatwirtschaftlicher Legende

In der chinesischen Botschaft wurden seitens der nachrichtendienstlich einzustufenden Militärabteilung Ermittlungen zu technischen Details und zum Hersteller einer Aufklärungsdrohne angestellt. Die Ergebnisse dürften anschließend nach China übermittelt worden sein. Eine Weile später erhielt die Herstellerfirma per E-Mail eine Anfrage einer chinesischen Firma zu ihren Produkten mit der Bitte, eine Delegation nach Deutschland entsenden zu dürfen, um erste Geschäftskontakte aufzunehmen.
Durch Ermittlungen in China stellte sich heraus, dass sowohl die chinesische Firma als auch die Person, die im Namen dieser Firma die E-Mail versandte, nicht existent war. Im vorliegenden Fall dürfte sich ein chinesischer vermutlich militärischer Nachrichtendienst einer privatwirtschaftlichen Legende bedient haben. Der Kontakt zu dem chinesischen Unternehmen wurde nicht erwidert.

Einbruch in Laptop bei Geschäftsreise in China

Die Leitungsebene der Forschungs-/Entwicklungsabteilung eines NRW-Unternehmens präsentierte ein neues Produkt in China per Laptop. Während einer Verhandlungspause wurde die deutsche Delegation gedrängt, die Räumlichkeiten zu verlassen, um kurzfristig die chinesische Unternehmensleitung begrüßen zu können. Nur der Leiter der Delegation war geistesgegenwärtig genug, sein Laptop zu sichern. Nach ca. einstündiger Rückkehr stellte die deutsche Delegation fest, dass versucht worden war, während ihrer Abwesenheit auf die Datenspeicher ihrer im Raum verbliebenen Notebooks zuzugreifen.

Laptopdiebstahl, chinesische Delegation

In einem weiteren Fall wurde ein neu entwickeltes Produkt einer deutschen Firma vor einer chinesischen Delegation mittels eines Laptops präsentiert. Kurz nach Abreise der Delegation wurde der Diebstahl des Laptops festgestellt. Neben den hochsensiblen Daten der Neuentwicklung befanden sich auch weitere wichtige Forschungsergebnisse des Unternehmens auf dem Laptop. Im Rahmen des Ermittlungs-/ Befragungsergebnisses stellte sich heraus, dass nur der Laptop mit den hochsensiblen Daten gestohlen worden war, obwohl noch weitere – modernere – Notebooks in dem Raum deponiert gewesen waren. Nach Angaben des Unternehmens eignen sich die gestohlenen Daten für einen Nachbau des Produkts, welches u.a. in der Raumfahrt- und Atomindustrie einsetzbar ist.
Aufgrund der Gesamtumstände ist davon auszugehen, dass es sich hierbei um einen gezielten Know-how Diebstahl gehandelt hat.

Proliferation

Was ist Proliferation?

Nach dem Ende des kalten Krieges hat sich die globale sicherheitspolitische Rahmenlage bekanntermaßen fundamental gewandelt; entgegen vielgehegter Erwartungen ist sie jedoch, wie wir mittlerweile wissen, nicht sicherer geworden. Um ihre politischen Absichten durchsetzen zu können, bemühen sich Länder aus bestimmten Krisenregionen bereits seit längerem darum, in den Besitz von nuklearen, biologischen oder chemischen Massenvernichtungswaffen und der zu ihrem Einsatz benötigten Trägertechnologie zu gelangen. Diese Weiterverbreitung von Massenvernichtungswaffen bzw. der zu ihrer Herstellung verwendeten Ausgangsprodukte, sowie von entsprechenden Waffenträgersystemen einschließlich der Bereitstellung des dafür erforderlichen

wissenschaftlichen und technischen Know-how bezeichnet man als Proliferation. Auch sog. Dual-Use-Güter, also Güter mit doppeltem, zivilen wie militärischen Verwendungszweck, fallen unter diese Begrifflichkeit.

Die Interessen der Beschafferländer

Staaten, die gegenwärtig nach der Verfügungsgewalt über Massenvernichtungswaffen streben, glauben, damit auf wie auch immer geartete außenpolitische Bedrohungen reagieren zu müssen und wollen eigene politische Forderungen gegenüber Nachbarstaaten oder der internationalen Staatengemeinschaft durchsetzen. Häufig fügt sich die forcierte Hochrüstung nahtlos in ein außenpolitisches Credo ein, das z.T. von Irrationalität und säbelrasselnder Kriegsrhetorik bestimmt wird. Mit dem Hinweis, im drohenden Konfliktfall „notfalls auch Massenvernichtungswaffen einzusetzen" errichten diese Staaten sicherheitspolitische Drohkulissen, die zugleich der Absicherung repressiver Machtstrukturen nach innen dienen, da die eigene Bevölkerung durch das Beschwören vermeintlicher äußerer Feinde von den zumeist gravierenden sozialen und ökonomischen Problemen der betreffenden Länder abgelenkt wird.

In diesem Zusammenhang bleibt auch die Bundesrepublik Deutschland weiterhin ein wichtiges Zielgebiet für Beschaffungsbemühungen verschiedener Problemländer, da bestimmte hochwertige Technologien und Know-how trotz verbesserter Infrastruktur in den Krisenländern und ungeachtet anderer Anbieterländer nur in den westlichen Industrienationen zu beziehen sind. Auch traditionell gewachsene Beziehungen können hierbei eine Rolle spielen.

Akteure

Zahlreiche Staaten vorwiegend aus dem sog. Islamischen Gürtel zwischen Marokko und Zentralasien sind in Deutschland aktiv, um proliferantionsrelevante Güter zu erwerben. Vor allem der Iran, Syrien und Pakistan entfalteten in den vergangenen Jahren erhebliche Aktivitäten in diesem Bereich. Daneben trat auch Nordkorea regelmäßig als Akteur in Erscheinung.

Die vorgenannten Staaten stützten ihre Proliferationsanstrengungen auf ihre Nachrichtendienste bzw. staatseigene Beschaffungsorganisationen ab, wobei verschiedenste verdeckte Methoden zur Anwendung kommen, die im folgenden noch Gegenstand näherer Betrachtung sein werden.

Methoden der Beschaffung

Massenvernichtungswaffen und die entsprechende Trägertechnologie sind auf den freien Märkten nicht erhältlich. Zum Schutz vor missbräuchlicher Weitergabe des einschlägigen Know-how gibt es in Deutschland neben strengen rechtlichen Rahmenbedingungen eine wirksame Exportkontrolle durch die zuständigen Behörden. Dennoch versuchen die o.g. Krisenländer, die hohen Hürden bei der Beschaffung sensibler Güter auf verschiedenstem Wege zu umgehen.

So erwerben sie die für sie interessanten Produkte mit Hilfe ihrer Geheimdienste, deren Mitarbeiter als Besteller oder Käufer agieren, bei z.T. exportunerfahrenen Lieferanten. Teilweise bedienen sie sich auch konspirativ arbeitender Beschaffungsnetzwerke oder geheimdienstlich gesteuerter Tarnfirmen, wobei das Vorschieben einer Handelsfirma zur Täuschung des Verkäufers über den steuernden Geheimdienst zu den klassischen Methoden zählt. Auch das Verschleiern der Endabnehmer durch den Gebrauch harmlos

klingender Firmennamen oder der Gebrauch neutraler oder irreführender Projektnamen für die Beschaffungsvorhaben gehören zum Standardrepertoire. Häufig werden als „Geschäftspartner“ für deutsche Firmen auch kleine Firmen im Ausland oder im eigenen Land gegründet, die lediglich der Abwicklung eines einzigen Geschäftes dienen und danach wieder geschlossen werden; als Drehscheibe für solche Geschäfte und Sitz solcher „Firmen“ wurden u.a. Singapur, Malta, Zypern oder Dubai festgestellt. Auch die Verschleierung des eigentlichen Endabnehmers von Proliferantionsprodukten durch den Export in vermeintlich „harmlose“ Länder, von wo aus die Ware über mehrere Stationen und Umwege über verschiedenen Zwischenhändler erst an ihren eigentlichen Bestimmungsort verbracht wird, ist ein häufig festzustellendes Verfahren bei der Beschaffung illegaler Rüstungsgüter. Typischerweise werden Beschaffungsvorhaben zudem in viele, für sich allein gesehen unverdächtige Einzelkäufe aufgeteilt, so dass der Proliferationshintergrund des gesamten Geschäftes nur schwer erkennbar ist.

Eine grundlegende Problematik besteht auch darin, daß es beim Export von Gütern, die zwar für zivile Zwecke deklariert sind, daneben aber auch noch militärisch genutzt werden können („Dual-Use-Güter“), fast unmöglich ist, eine missbräuchliche Verwendung durch den Endabnehmer auszuschließen. So können beispielsweise Chemikalien, die vornehmlich in der Landwirtschaft oder der Pharmazie Verwendung finden, in anderer stofflichen Zusammensetzung als chemische oder biologische Kampfstoffe zum Einsatz gebracht werden.

Fallbeispiel

Das folgende Fallbeispiel aus Thüringen illustriert die mögliche Vorgehensweise eines Krisenstaates bei der Beschaffung rüstungsrelevanter Industriegüter in der Bundesrepublik Deutschland.

Im Dezember 2004 erhielten deutsche Stellen einen Hinweis aus den VAE, dass ein aus Hamburg kommendes Schiff mit proliferationsrelevanten Gütern, die mutmaßlich für ein iranisches Raketenprogramm bestimmt waren, durchsucht worden war. Bei der Maßnahme wurden u.a. Teile einer Vibrationstestanlage gefunden, die von einer Firma aus dem Südthüringer Raum hergestellt und vertrieben werden. Als Zwischenhändler trat eine chinesische Firma auf, die als Umweglieferant für das pakistanische Nuklearprogramm bekannt war. Der Empfänger in den VAE war eine Firma in Dubai, die wiederum als getarnte Beschaffungsstelle für das iranische Trägerraketenprogramm gilt und bereits Gegenstand von Ermittlungen der VAE-Behörden war. Ihr Geschäftsführer wurde im Dezember 2004 in Europa wegen illegalen Waffenhandels verhaftet. Diese mutmaßliche iranische Tarnfirma hatte im Laufe des Jahres 2004 im Rahmen gezielt aufgebauter Kontakte zum Geschäftsführer und einem verantwortlichen Exportmitarbeiter des Thüringer Spezialmaschinenherstellers die o.e. Vibrationstestanlage erworben, mit denen u.a. die Funktionsfähigkeit von Raketenturbinen getestet werden kann. Die Geschäftskontakte zwischen der Firma in Thüringen und den für den Kauf zuständigen iranischen Stellen reichten jedoch schon einige Jahre zurück. Aufgrund der belastenden Hinweise und nach weiteren Ermittlungen wurden die beiden genannten Personen im April 2005 festgenommen sowie Firmen- und Wohnräume durchsucht. Gegen die Festgenommenen richtete sich der Vorwurf der geheimdienstlichen Agententätigkeit sowie des Verstoßes gegen das Außenwirtschaftsgesetz. Nachdem der Vorwurf der geheimdienstlichen Agententätigkeit fallengelassen wurde, verhängte das Gericht gegen den ehemaligen Geschäftsführer der Firma eine Haftstrafe von 23 Monaten auf Bewährung sowie eine Geldbuße in Höhe von 50.000 €; sein Mitangeklagter, der ehemalige Exportchef des Unternehmens, musste eine Geldbuße von 5.000 € bezahlen und erhielt überdies eine 16-monatige Bewährungsstrafe. Darüber hinaus wurde gegen die betroffene Firma eine Geldbuße von 20.000 € verhängt.

Durch die Kombination von Scheinfirmen mit geheimdienstlichem Hintergrund, des mehrfachen Einsatzes von Zwischenhändlern, dem gezielten Verschleiern von Transportwegen und Endabnehmern sowie dem Auftreten von Vertretern staatlicher Handelsorganisationen als „Käufer“ ist dieser Fall ein „klassisches“ Beispiel für die konspirativen Beschaffungsmethoden der Nachrichtendienste von Krisenländern, die weder Aufwand noch Kosten scheuen, um sich in den Besitz von illegalem Know-how zu bringen.

Fazit

Wirtschaftsspionage schädigt unsere nationalen wirtschaftlichen Strukturen und volkswirtschaftlichen Interessen in unverändert hohem Maße, wohingegen Proliferation die friedlichen internationalen Beziehungen wie auch die Bemühungen, Konflikte einzudämmen und zu verhindern, gefährdet. Beides ist für ein Land, das seine internationale Geltungskraft aus ökonomischer Prosperität und dem vielfach bewiesenen Willen zur Gestaltung einer Weltfriedensordnung bezieht, nicht hinnehmbar. Zwar ist die Abwehr von illegaler Ausforschung im Wirtschaftsbereich und der verdeckten Beschaffung von Hochrisikogütern durch Krisenländer aufgrund verfeinerter Methoden der Gegenseite schwieriger geworden, doch sie ist nicht aussichtslos. Voraussetzungen einer erfolgreichen Abwehr sind: Sensibilität gegenüber den Angriffsgefahren, Kenntnisse über die Methoden und Ziele der Nachrichtendienste, der Einsatz geeigneter Schutzmaßnahmen und die Einsicht in deren Notwendigkeit. Um diese Voraussetzungen zu schaffen und Ihnen, meine Damen und Herren, praktische Hilfestellungen bei der Bewältigung möglicher Verdachtsfälle zu leisten, stehen Ihnen das Thüringer Landesamt für Verfassungsschutz sowie das Thüringer Landeskriminalamt im Rahmen ihrer gesetzlichen Befugnisse weiterhin zur Verfügung.

China: Im Haifischbecken schwimmen lernen

Dr. Andreas Blume, Leiter Kompetenzzentrum VR China der IHK Pfalz, Ludwigshafen

Sehr geehrte Damen und Herren,

der Titel meines Power-Point-Vortrages ist bewusst sehr provokativ gewählt. Damit möchte ich auf die vielfältigen „Stolperstellen“ aber auch die Möglichkeiten im Umgang mit Partner aus Fernost und speziell aus China hinweisen.

IHK Pfalz
Kompetenzzentrum China

Spionage,
Produkt- und Markenpiraterie und
„phantasievolle“ Know-how-Akquise –

was auf Unternehmen zukommt, wie man sich darauf einstellen sollte

Im Haifischbecken schwimmen lernen

IHK Pfalz
Kompetenzzentrum China

Haifischbecken China

Gibt es eine Gemeinsamkeit?

© Andreas Blume 2006

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Haifischbecken China

- **Bsp:** General Motors beklagt Kopien seines PKW „Spark“ bzw. „Daewoo Matiz“ durch das Staatsunternehmen Chery, Chery QQ ist „Klon“ von diesen Fahrzeugen. Hier gingen Blaupausen „verlustig“...

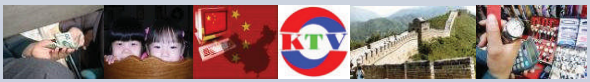

- **Gefahr für Know-how: Weshalb China? Kombination aus:**
  - Kein Rechtsstaat
  - Spionage + Produktpiraterie gehen Hand in Hand
  - äußerst findige Geschäftsleute / Ehrgeiz / Netzwerke
  - Kontrollverlust Pekings (partiell)
  - strategische Industriepolitik / Branchen
  - Gekonnter Umgang mit Taktiken & Strategien u.v.m.

IHK Pfalz Kompetenzzentrum China

Übersicht über Workshop

Teil I: Umfeld & Hintergründe

1. Einstieg und Rahmenbedingungen
2. Wirtschaftsspionage – Abriss
3. Know-how Abfluss: Gesetzl. Bestimmungen
4. Produktpiraterie und das chinesische IP-Regime
5. Lokale Akteure – „der Himmel ist hoch und Peking weit weg“
6. Gezielte Taktiken auf individueller oder Unternehmens-Ebene



Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Übersicht über Workshop

Teil II: Strategische Überlegungen/Maßnahmen

8. Technologietransfer nach China: allgemeine Erwägungen / Maßnahmen
9. Maßnahmen im Bereich des Geheimschutzes
10. IP-Schutzmaßnahmen

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Teil I: Umfeld & Hintergründe

Ohne Kenntnis des Umfeldes und der Hintergründe des organisierten Multi-Level-Know-how-Abflusses in China ist eine realistische Einschätzung der Situation und eine den Herausforderungen angemessene Strategieentwicklung nicht möglich!

Im Haifischbecken schwimmen lernen

IHK Pfalz
Kompetenzzentrum China

1. Einstieg

- **Öffnung Chinas unter Deng Xiaoping ab 1978:**

„Es ist egal, welche Farbe die Katze hat, Hauptsache Sie fängt Mäuse!“

„Es ist egal, welche Mittel wir anwenden, Hauptsache China wird stark!“
No level playing field!

Misstrauen gegenüber westlichen Akteuren und Unternehmen war und ist z.T. immer noch in den Köpfen chinesischer Funktionäre.

- Chinesen müssen Herr über ihre Wirtschaft bleiben!
- „Staatsgelenkter industriepolitischer Turbokapitalismus“

IHK Pfalz
Kompetenzzentrum China

Einstieg

- **China heute:**

- seit 1978 bis heute stetiges durchschnittliches **Realwachstum von 9,5% p.a.**
- Ein nicht unbeachtlicher Teil dieses Wirtschaftswachstums ist auf den Missbrauch geistiger Eigentumsrechte und den Diebstahl von Betriebs- und Geschäftsgeheimnissen zurückzuführen. → ***Teufelskreis!***
- Chinas Volkswirtschaft = Nr. 5 weltweit, 2,3 Bill. US$ BSP
- China ist **bereits drittgrößte Handelsnation** und wird mit Deutschland im Jahre 2007 gleichziehen
- **Chinas Beitrag** zum Wachstum der Weltwirtschaft: > 12% (2005)

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Einstieg

- **Hintergründe für Know-how-Bedarf = derzeitig größte Aufgabe der Führung des Einparteienstaates:**

um jeden Preis!

Wirtschaftswachstum muss aufrecht erhalten werden, darf nicht unter 7% p.a. fallen: ideologisches Vakuum.

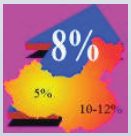
„Grow or Die“: Überlebensfrage der KPCh

IHK Pfalz Kompetenzzentrum China

Einstieg

- Da die weltweite Marktdurchdringung von chinesischen Verbrauchs- und Gebrauchsgütern einfacher Qualität und Güte bereits weit fortgeschritten ist und nur noch wenig Wachstumspotential bietet, wird verstärkt auf **technologisches Upgrading** gesetzt, um die Wachstumsmaschinerie am Leben zu halten.

- Chinas historische Machtposition „reinstallieren“ Daher: **besonderer Nährboden für professionellen Know-how-Diebstahl** auf vielen Ebenen und in vielfältiger Form und Ausprägung.



IHK Pfalz Kompetenzzentrum China

Ergänzungen

2. Wirtschaftsspionage

Staatsziele:

- bis spätestens 2020 **führende Weltwirtschaftsmacht** werden
- Schaffung einer Wissenschafts- und Technikarmee zum Aufbau Chinas (Technologieentwicklungspläne 863, 973, Falkenplan, Funkenplan – mit jeweils nachrichtendienstlicher Komponente)
- **Technologierückstand verringern**
- (Technische) **Bildung wird als äußerst wichtig betrachtet**:

→ fast alle Mitglieder des Ständigen Ausschuss des Politbüros haben Ingenieurstudium absolviert

→ „Xiaomei ist unsere Fahrkarte für ein besseres Leben“

→ „Bildung beeinflusst Dein Schicksal“ (Chin. Sprichwort)

IHK Pfalz Kompetenzzentrum China

Wirtschaftsspionage

Vorgehensweise chinesischer Nachrichtendienste:

- Es werden **Mitarbeiter chinesischer Nachrichtendienste** gezielt in deutsche Universitäten oder Unternehmen mit Hochtechnologie bzw. mit „gewünschter Technologie“ eingeschleust: Praktikanten, Diplomanden, Doktoranden.
- **Normalmodus** chinesischer Studenten: 6-7 Semester scheinfrei!
- **Auffällig:** Studenten, die genauso lange wie Deutsche studieren und ein Praktikum nach dem anderen in „interessanten Firmen“ absolvieren.

IHK Pfalz Kompetenzzentrum China

Wirtschaftsspionage

Vorgehensweise chinesischer Nachrichtendienste:

- **Besonders betroffene Branchen:**

KFZ, Eisenbahn, Luftfahrt, Bio- und Gentechnologie, Medizintechnik, chemische Industrie, pharmazeutische Industrie, (Spezial-)Maschinenbau

→ überall dort, wo Deutschland noch „**Tafelsilber**“ zu verschenken hat

→ **strategische Entwicklungsbranchen Chinas**

→ Anfällig für nachrichtendienstliche Unterwanderung

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Wirtschaftsspionage

Vorgehensweise chinesischer Nachrichtendienste:

- Ausspähen von ausgestellten **Maschinen auf Messen**
  Gezielte nachrichtendienstliche Führung der Spione.
- **Internetüberwachung**
  - Ca. 50.000 Internet-Überwacher von Chinas Regierung eingesetzt

  - Weitreichende Überprüfungs-, Sperrungs- und Lesemöglichkeiten vorhanden. Technik, Mails auf bestimmte Inhalte hin zu untersuchen und einzelne Empfänger oder Absender anzuvisieren.
  - Mitarbeiter des MSS besuchen Uni-Seminare (Ingenieurs-, Natur- und Wirtschaftswissenschaften) um zu lernen, nach welchen Begriffen sie fahnden müssen.

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Wirtschaftsspionage

Vorgehensweise chinesischer Nachrichtendienste:

- Aber es werden auch **infame Methoden** angewandt:
  - Wenn pot. Informant nicht kooperationswillig, dann Erzeugung von **Kompromat**, um ihn unter Druck zu setzen, z.B. Bordellbesuche von Familienvätern.

  - Vorgabe, man sei von **chinesischen Triaden** und nicht von den chinesischen Sicherheitsdiensten... Angst wird geschürt...

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

3. Gesetzliche Regelungen Lizenzen

- **Neue Regelungen (ab 2002)**

  - Einteilung in **verbotene, beschränkte** und **unbeschränkte** Lizenzgeschäfte
  - Jetzt: Nicht mehr jedes Lizenzgeschäft ist genehmigungspflichtig, bleibt aber registrierungspflichtig

Problem #1: wenn das Projekt in falsche Kategorie subsumiert wird / Exklusive Lizenzen

→ Lizenzvertrag wird unwirksam
→ rechtl. Grundlage zur Zahlung Lizenzgebühr entfällt, selbst wenn Technologie schon genutzt wird.
→ Es scheint, als ob dieses Problem „gefördert“ wird.

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Gesetzliche Regelungen Lizenzen

Problem #2: Gelebte Praxis der Lizenznahme!

- → Ihr liz. Know-how wird an Dritte weitergegeben
- → Rechtl. Mögliches Verbot, lizenzierte Technologie nach Ablauf des Lizenzvertrages nicht mehr zu nutzen, ist in Praxis nicht durchsetzbar
- → Überproduktion: Overnight & Weekend, Norm?!
- → Verkauf von Ausschussteilen
- → Ausleihen von Maschinen und Prüfgeräten
- → Verkauf von Zulieferteilen an die Konkurrenz
- → Illegales Upgraden von Produkten des chin. Unternehmens

Merke: *Wer vitales Know-how in Form einer Lizenz nach China ohne „Sollbruchstellen" vergibt, ist sehr mutig...*

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Gesetzliche Regelungen Investment Guidance Catalogue

- **IGC regelt Investment** nach Branchen, 100%ige Tochter oder nur Joint Venture möglich?
- Aktuelle Version des IGC vom 30.11.2004
- *Aber:* Grundsatz, alle Investitionsprojekte unterliegen der Genehmigung durch chinesische Behörden.
- Steuerferien für „encouraged categories": ND haben Zugriff auf Steuerbehörden, Offenlegung des Vorhabens
  → neue Angriffspunkte für ND

Problem #1: In manchen Bereichen JV-Gründung immer noch vorgeschrieben

- KFZ: max. zulässiger ausländischer Anteil: 50%
- Schienenfahrzeuge: Lokalisierungspflicht von 70%

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Gesetzliche Regelungen IGC

Problem #2: Missbrauch durch interne Vorschriften

- Projekt ist zwar laut IGC als 100%ige Tochter erlaubt, wird aufgrund interner Vorschriften nur als Joint Venture genehmigt
- Bsp: Eisenbahnsektor: Zulieferer

→ Chinesische Zentralregierung **setzt gezielt** das Instrumentarium **Joint Venture** ein, um an fremdes Know-how zu gelangen

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Gesetzliche Regelungen IGC

Problem #3: Gezielte JV-Substitution

- **Ziele des dt. Unternehmens**: Kostenniveau senken, dadurch Wettbewerbsfähigkeit steigern, chinesischen Markt erschließen, ggfs. exportieren
- **Ziele des chin. Partners:** Unliebsames Personal entsorgen, an Finanzmittel gelangen, an Know-how kommen, nicht nur technisches Wissen, sondern auch Vertriebs-, Marketing- und Management Know-how

- **Vorsicht Camouflage!** 2-3 Jahre überaus kooperatives Verhalten, Vertrauen gewinnen, bis relevantes Know-how abgeflossen ist.
  Dann: eigene Produktion aufbauen, Know-how auf eigene nutzen, JV versanden lassen

Die Gründung eines Joint Adventures ist nur in Ausnahmefällen sinnvoll!

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Gesetzliche Regelungen Zertifizierungen

- Seit 1.5.02 gilt die neue **CCC-Zertifizierung** in China, ist zwingend vorgeschrieben für Importe und lokal hergestellte Produkte
- CCC-Pflicht umfasst 19 Produktgruppen und 132 Produktkategorien, vor allen Dingen „technologisch Interessantes"
- Zertifizierungen sind eine „normale Sache", wenn sichergestellt wird, dass Know-how, das offen gelegt werden muss, nicht abfließt und von Dritten missbraucht wird.
- Zuständigkeit: China Quality Certification Centre (CQC), Testlabors, (reisende) Auditoren, die eine **Werksinspektion in Deutschland durchführen.**

IHK Pfalz Kompetenzzentrum China

Gesetzliche Regelungen Zertifizierungen

- Know-how auf dem **Präsentierteller**?
- Berichten betroffener Unternehmen zufolge, muss alles offengelegt werden: umfangreiche technische Dokumentationen, Produktmuster, Mustergeräte, usw.
- **Know-how floss bereits in einigen Fällen nachweislich ab**:

  - Dt. Hersteller von Elektromotoren: „halbjährige Zertifizierung, Ansprechpartner haben ständig gewechselt, geschäftsinterne Akten und Konstruktionspläne mussten vorgelegt werden, sogar Mustergeräte zur Prüfung überlassen werden, nach 1,5 Jahren perfekte Kopie von chinesischem Hersteller auf der Hannover Messe."

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Gesetzliche Regelungen Verschlüsselungstechnik

- **offiziell nur chinesische Verschlüsselungstechnik / Software erlaubt** (Quellcodes sind hinterlegt...!)
- **VPN wir manchmal lokal „genehmigt“,** dann zentral abgeschalten
- **Wer verschlüsselt telefoniert, bekommt Besuch...**
- **Shenzhener Hammer...**
- **„Mittelalterliche Lösungsansätze“:** Serienbriefe, Buchstabenverschlüsselungen wie vor 2. WK „Alles außer ITK“

IHK Pfalz Kompetenzzentrum China

Gesetzliche Regelungen Designinstitute

- **Produktionsaufbau: Zwang chinesische Designinstitute einzuschalten**
  - Beim Entwurf ganzer Fabriken und Produktionsanlagen, insbesondere in der chemischen Industrie, müssen chinesische Designinstitute eingeschalten werden. Dabei wird **zwangsläufig Know-how** über Technologien als auch über Projektabwicklungen **transferiert**.
  - **Verschärft wird Situation** durch:
    -- hohe Fluktuation der chinesischen Ingenieure
    -- vorgeschriebene Dokumentation der Planungen verbleibt nicht im Eigentum des Auftraggebers
    -- Chin. Designinstitute bieten mit ihrem illegal erworbenen Wissen ihre Dienste auch Wettbewerbern des urspr. Auftraggebers an.
    -- treten auch in großem Stil selbst als Produzenten auf

Im Haifischbecken schwimmen lernen

IHK Pfalz
Kompetenzzentrum China

Manch deutscher Maschinen- und Anlagenbauer kann sich recht schnell ungefähr so fühlen...

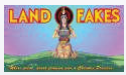
Im Haifischbecken schwimmen lernen

IHK Pfalz
Kompetenzzentrum China

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

4. Paradies für Produktpiraten - das IP-Regime Chinas



- **Hintergrund:** China als Land mit den größten und umfangreichsten IP-Verletzungen in der Geschichte der Menschheit!
- Ca. 10% des Welthandels sind „fake“, davon stammen 60% aus der VR China, Marktdurchdringung in China: 60%
- „**In China ist nur Deine Mutter echt**“ – es wird **alles** gefälscht:

  Uhren, Textilien, Parfums, Elektrowerkzeuge, Lötgeräte, elektronische Produkte, Klimaanlagen, Druckerpatronen, Mobiltelefone, Batterien, Radarwarner, Aufzüge und Teile davon, Musikinstrumente, Zubehör z.B. Notenständer, Saiten, Saitenhalter, KFZ-Ersatzteile und KFZ-Ausrüstungen wie Felgen, Bremsbeläge und –scheiben, Kurbelwellen, Fußmatten, Zylinderköpfe, Windschutzscheiben, außerdem: Nahrungs- und Genußmittel, Spielwaren und Babyartikel (verseuchte Schnuller), gesamte Straßenbahnen und Automobile, gefälschte Militär- und Polizeiuniformen

  Außerdem: Ganze Geschäfte, Maschinen & Anlagen, Fabriken und Medikamente!

IHK Pfalz Kompetenzzentrum China

Das Counterfeiting-Ausmaß

- **Umfrage der IHK Pfalz (11/2004): Produktpiraterie in und aus China**

  52 Unternehmen antworteten (fünfseitiger Fragebogen)

  … sind 56% Opfer von Markenverletzungen
  … melden 35% Patentverletzungen
  … berichten 27% über Geschmacksmuster-verletzungen
  … geben 13% Vergehen gegen das Urheberrecht an

  77% der Rückläufer haben Probleme mit ihren IP-Rights in China

IHK Pfalz
Kompetenzzentrum China

Das Counterfeiting-Ausmaß

- **Umfrage der IHK Pfalz (11/2004)**

Hat sich die Fälscheraktivität innerhalb der letzten zwei Jahre verändert?

verringert: 3%

keine nennswerten Änderungen: 22%

vergrößert: 75%

IHK Pfalz
Kompetenzzentrum China

Das Counterfeiting-Ausmaß

- **„IP-Dumping“:**

- Was nach internen Auskünften **regelrecht Strategie** zu sein scheint:
  - → Optisch gute Fälschung wird absichtlich qualitativ schlecht produziert, obwohl man es besser könnte, um Marke zu beschädigen (Reputationsverlust).

    Aufbau einer Marke: ist aufwändig, langwierig, teuer
    Beschädigung einer Marke ist schnell und einfach

    Dann wird mit Plagiaten an Preisschraube gedreht, Konkurrenz soll aus dem Markt geschossen werden.

Im Haifischbecken schwimmen lernen

IHK Pfalz

Das Counterfeiting-Ausmaß

- Ein konkretes Indiz für den hohen Organisationsgrad der Fälscher ist die **große Geschwindigkeit**, mit der Innovationen ausgebeutet und zu eigenen Gunsten in großem Stil versilbert werden.

- Es bestehen regelrechte **Fake-Outlet-Centres**, d.h. gefälschte Muster werden in allen möglichen Varianten ausgestellt, die dann bestellt werden können.

Im Haifischbecken schwimmen lernen

IHK Pfalz

Das Counterfeiting-Ausmaß

Fälscher agieren häufig schneller als Originalhersteller...

- Um einen x-beliebigen Sportschuh zu reproduzieren, benötigen chinesische Netzwerke **rund 10 Tage** für **1.000 Paar Schuhe zu einem Preis von rund 4 US$.**
  → Re-engineering – Materialeinkauf - Produktion

Nachfrageorientiertes System - kaum Unterschiede zu legaler Produktion

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Das Counterfeiting-Ausmaß

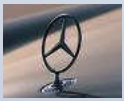
- ***Bsp. Daimler-Chrysler:***

  - gefälschte Ersatzteile aller Art,
    Windschutzscheiben, Bremsscheiben, Bremsbeläge
    Marktanteil gefälschter Kfz-Teile in China: 30-70%

  - **Bus-JV** in Yangzhou (ab 1997)

  - Designkopie: **Geely MR 300**
    Front C Klasse, Heck 5-er BMW, Smart

  - Dienstleistungsfälschung: **Gefälschte Werkstätten**



IHK Pfalz Kompetenzzentrum China

Das Counterfeiting-Ausmaß

- Anti-Baby-Pillen aus Milchpulver
- Herzmedikamente ohne Wirkstoff
- Asthma-Sprays mit Kerosin
- Fenfluramin verseuchte Diät-Pillen

- Tragisch: Schätzungen zufolge **starben letztes Jahr rund 200.000 Menschen** in China an gefälschten Medikamenten und Nahrungsmitteln.
  Und in Afrika Mio. Menschen an gefälschten chinesischen (HIV-)Medikamenten!

IHK Pfalz Kompetenzzentrum China

Das IP-Regime Chinas

- **Wer profitiert heute von Chinas IP-Regime?**

➔ Der **Rechtsverletzer** und die **rechtsdurchsetzenden Behörden**, **nicht aber der Rechtsinhaber**!

Anreizstruktur für Rechtsverletzer: ***äußerst positiv***

- exorbitant hohe Gewinne
- schnelle Umsätze
- verschwindend geringe Wahrscheinlichkeit, entdeckt zu werden
- Möglichkeit, durch Einflussnahme, persönl. Beziehungen, Bestechung oder Verbrüderung sich einer Strafe zu entziehen
- Milde Strafen, keine Mindeststrafen vorhanden

IHK Pfalz Kompetenzzentrum China

Das IP-Regime Chinas

Anreizstruktur für Rechtsinhaber:
sehr negativ

- Hürden der Schutzrechtsanmeldung
- Kollidierende Marken, fremde Rechtsanmeldungen
- keine Unterstützung durch Behörden
- muss teure Detektive beschäftigen (manchmal mit eigener Agenda..)
- überzogene Anforderungen an Beweise
- Zahlung einer hohen „Case Fee“
- hohes Maß an Intransparenz bei den Verfahren
- Absprachen zwischen Behörden und Rechtsverletzer
- unklarer Ausgang des Verfahrens, i.d.R. keine Kostenerstattung / nennenswerten Schadensersatz

IHK Pfalz
Kompetenzzentrum China

Das IP-Regime Chinas

Anreizstruktur für Behörde: *positiv*

- Verwaltungsverfahren (Case Fee und zusätzliche Sonderzuwendungen)
- bei Gerichtsverfahren häufig Bestechungsgelder –
  Wie erkennen Sie einen ehrlichen Richter in China?
- Behörde verfügt über großen Manipulationsspielraum, um betroffene Akteure in ihrem zuständigen Gebiet entweder gegen Gegenleistung zu protegieren oder unter Druck zu setzen
- Häufig rangeln unterschiedliche Behörden um Zuständigkeit, um Macht, Einfluss und Einnahmen (auch individuelle) zu erhöhen

State Intellectual Property Office of the P.R.C

Im Haifischbecken schwimmen lernen

IHK Pfalz
Kompetenzzentrum China

Abwehrmaßnahmen der Fälscher

"Counter-Anti-Counterfeiting"

Just waitin' for countering your countermeasures!

- Fabrikcluster für politischen Schutz
- Anmietung von Appartments
- Blanks, Thermodrucker anbei
- Hightech-Fälschungen
- Preispolitik der Fälscher
- Gezielte Desinformation
- Vertrieb von Kleinsendungen
- Verschleierung der Transportwege
- Einfuhr der Ware in die EU über GR
- Fakes-Großmärkte in Polen/Tschechien
- Fälschung von Ursprungszeugnissen
- Fremdanmeldung von IP-Rechten, etc.

Im Haifischbecken schwimmen lernen

IHK Pfalz
Kompetenzzentrum China

5. Lokale Akteure

- **Direkt oder indirekt lokalstaatlich gelenkte Wirtschaftsspionage im Mantel der Industriespionage**

  Know-how-Akquise geht nicht nur von Peking aus!

  → Chinesische Industriestruktur:

  kompliziertes Geflecht territorial abgestufter Eigentumsrechte, das nur noch in strategischen Bereichen der chinesischen Volkswirtschaft zentralstaatlicher Kontrolle unterliegt.



IHK Pfalz
Kompetenzzentrum China

Lokale Akteure

- **Local State Corporatism**

  - entwickelte sich auf Basis der Dezentralisierung ab 1956
  - Regierungen auf lokaler Ebene (Kreis, Gemeinden, Dörfer) behandeln die ihnen unterstellen Unternehmen als **Teil einer übergreifenden Konzernstruktur**:

Kreisregierung:	Corporate Headquarters
Gemeinderegierung:	Regional Headquarters
Dörfer:	Profit Center

  - **Eisernes Interessengeflecht** zwischen Partei, Lokalregierungen, Unternehmen, Gerichte, Staatsanwaltschaft und Polizei

Im Haifischbecken schwimmen lernen

IHK Pfalz

Lokale Akteure

- **Local State Corporatism**
  - Jede Organisationsebene ist finanziell auf sich selbst gestellt, operiert unter harter Budgetrestriktion und die **Einkommen der Funktionärsschicht hängen direkt von der Ertragskraft der örtlichen Betriebe ab.**
  - Dabei handeln dezentrale Politiker aus einem Anreizsystem heraus, dem gemäß sie in erster Linie darum bemüht sind, **Wirtschaftswachstum, Arbeitsplätze und Steuereinnahmen** zu maximieren. Sollten Anweisungen der Zentrale diesen Zielen zuwiderlaufen, werden häufig Verschleppungs- oder Umgehungstaktiken bemüht.
  - *„Shang you zhengce, xia you duice!“*

- Und: Kader & Bürgermeister **selbst Anteilseigner an** Unternehmen; **initiieren** Spionage und Produktpiraterie

IHK Pfalz

6. Gezielte Taktiken

- **„First-to-File“: Wie Originalhersteller zu Produktpiraten werden**
  - Chinesische Produktpiraten versuchen Inhaber gewerblicher Schutzrechte mit den eigenen Waffen zu schlagen:→ **Anmeldung fremder Marken und Patente** (auch Gebrauchsmuster und Geschmacksmuster) identisch oder leicht modifiziert auf eigenen Namen an.
  - **„Auslöse“ erzwingen**
  - **„Schonfrist“ nutzen**
  - „Schonfrist“ für viele Unternehmen = „Galgenfrist“

IHK Pfalz Kompetenzzentrum China

Gezielte Taktiken

- **Spezielle Verbrüderungstaktiken um Warnsysteme“ ausländischer GF „auszuschalten“**

- aufwändige Bankette
- Lob und Schmeicheleien
- Ständiges Betonen von Freundschaft
- Gemeinsames „Saufen“
- Singlallen... Gemeinsame Besuche in Karaoke-Bars
- Gemeinsame Bordellbesuche, ggfs. Kompromat
- Know-how-Trägern wird „Überlauf“ mit phantastischen Konditionen angeboten

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Gezielte Taktiken

- **Exkurs: der deutsche Geschäftsmann**

- Ehrlichkeit und Verlässlichkeit
- steht zu seinem einmal gegebenen Wort
- artikuliert seine Bedürfnisse klar
- trägt Konflikte aus, um Probleme aus der Welt zu schaffen
- **Ideal: Fair Play**
- Innovation
- Vertragsgetreue Geschäftsbeziehung

„Lass Dich nicht biegen, auch wenn es dabei zum Bruch kommt.“

Symbol: Fels in der Brandung

Spiel mit ungleichen Karten!

Im Haifischbecken schwimmen lernen

IHK Pfalz
Kompetenzzentrum China

Gezielte Taktiken

• **Exkurs: der chinesische Geschäftsmann**

- Freundlichkeit und Höflichkeit
- gesichtswahrende Kommunikation
- **Ideal: Schlitzohrigkeit**; denn dies ist unumgänglich, um sich im Geschäftsleben zu behaupten
- Umgang mit Situationen, Ursachen und Fehler werden nur selten analysiert
- Es zählt die Beziehung zum Geschäftspartner, nicht der Vertrag: Flexibilität
- Nachverhandeln als Norm
- Reproduktion

„Lass Dich biegen, aber lass es nicht zum Bruch kommen."

Symbol: Bambus

IHK Pfalz
Kompetenzzentrum China

Gezielte Taktiken

• **Spezielle Verhandlungstaktiken:**

- Chinesische Verhandlungspartner beherrschen **klassische Verhandlungstaktiken**:

36 Strategeme
= Kriegslisten von General Tan Daoji

Strategem Nr. 7: Aus dem Nichts etwas erzeugen
→ *Durch Vorgaukeln eines Trugbildes sich einen Vorteil verschaffen*
→ *Sich selbst als perfekten JV-Partner präsentieren, um an Know-how zu gelangen:*

- Gerüchte streuen
- falsche Unternehmen präsentieren
- Kunden werden erfunden
- Bilanzen werden beschönigt
- Zertifizierungen werden gefälscht

IHK Pfalz Kompetenzzentrum China

Gezielte Taktiken

- **Spezielle Verhandlungstaktiken:**

Strategem Nr. 15: Den Tiger bewegen, die Berge zu verlassen

→ *Den Opponenten dazu veranlassen, sein angestammtes, vertrautes und für ihn günstiges Terrain zu verlassen:*

- Verhandlungen in China und nicht in Deutschland durchführen
- Nutzung eines selbst entworfenen, parteiischen „Standardvertrages“

Die Kunst des Krieges, Meisterwerk Sunzis

→ Wenn Du Dich und Deinen Feind kennst, brauchst Du den Ausgang von 100 Schlachten nicht zu fürchten!“

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Gezielte Taktiken

- **Spezielle Verhandlungstaktiken:**

- Gesichtswahren wird als Verhandlungstaktik eingesetzt!

Zugeständnisse werden erheischt, danach wird darauf gebaut...

- Vorschriften werden erfunden, um eigene Ziele zu erreichen

- Förderung der selektiven Wahrnehmung durch getürkte Daten...

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Gezielte Taktiken

Glücks-Ritter auf dem Weg zu mehr Know-how

- eines der **ganz großen Probleme** deutscher Unternehmen in China – **extrem hohe Mitarbeiterfluktuation,** 1/3 der leitenden Angestellten wechselt innerhalb Jahresfrist.
- Gehälter werden intensiv kommuniziert
- **Loyalität zu Unternehmen**? Fremdwort! Eigennutz! Selbständige Nebentätigkeiten, die jedoch mit der Hauptarbeit im Angestelltenverhältnis direkt korrespondieren = **Normalzustand**
- Gezieltes Ausnutzen des Arbeitsverhältnisses, um auf eigene Rechnung zu arbeiten.
- Innere Kündigung kann zur Gefahr werden → ***Mafan!***

IHK Pfalz Kompetenzzentrum China

Wer in China langfristig Erfolg haben will und sein Unternehmen nicht durch ein China-Engagement in seiner Existenz gefährden will, muss...

A) Die **Gefährdungslage** genau kennen

B) Auf dieser Basis **strategische Entscheidungen** unternehmens- und produktspezifisch fällen

C) Dann ein **Schutz-Maßnahmenkatalog** erarbeiten und diesen unter Kosten-Nutzen-Erwägungen umsetzen.

Meist findet A) und C) nicht ausreichend Berücksichtigung!

IHK Pfalz Kompetenzzentrum China

Im Haifischbecken schwimmen lernen

Teil II:

Strategische Überlegungen und Maßnahmen

IHK Pfalz Kompetenzzentrum China

Im Haifischbecken schwimmen lernen

8. Allgemeine Erwägungen

Grundsätzliche Fragen:

Wie muss der **Zielkonflikt** zwischen **strategischer Erschließung neuer Märkte und Know-how-Schutz** gewichtet werden, um die Unternehmensentwicklung **nachhaltig** zu gestalten?

Und: **Gibt es risikoärmere Alternativen zu China?**

© Andreas Blume 2006

IHK Pfalz Kompetenzzentrum China

Allgemeine Erwägungen

Welche Faktoren abwägen und berücksichtigen?

- Befindet sich das angestrebte Projekt in einer „**strategischen Entwicklungsbranche**“ der chinesischen Zentralregierung?
  → besonders hohes Risiko nachrichtendienstlicher Unterwanderung
- Darf eine **100%ige Tochter**, ein Mehrheits- oder nur ein Minderheits-JV gegründet werden?
- Wie hoch sind die Vorschriften des **local content**?
- Hängt das Projekt vom Zuschlag im Rahmen einer **Ausschreibung** ab?
- Ist der Erfolg des Projektes **alleine** oder nur in einem Konsortium realisierbar?

IHK Pfalz Kompetenzzentrum China

Allgemeine Erwägungen

Welche Faktoren abwägen und berücksichtigen?

- **Kundenstruktur:** Staatsunternehmen oder private Unternehmen
- **Anzahl** potentieller Kunden
- **Eigenvertrieb** (selektiver Vertrieb) oder Vertrieb über Mittler
- Eigene **Fertigungsstiefe** in China, Wertschöpfung
- Zuverlässigkeit der **Zulieferer**
- **Länge der Nutzungsdauer**
- Stand im **Produktlebenszyklus**
- **Preis**niveau und Preisentwicklung
  → Amortisation des Projektes vor Substitution

© Andreas Blume 2006

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Allgemeine Erwägungen

Welche Faktoren abwägen und berücksichtigen?

- Ist Produkt international marktfähig? D.h. ist **Export** geplant oder zu befürchten?
- Welche Produktlinien und **Technologien** sollen transferiert werden?
- Sind **Rückfallpositionen** vorhanden?
  z.B. Transfer der „classic line“ und nicht der „innovative line“
- Können **Sollbruchstellen** eingebaut werden?
  → Wertschöpfungskette unterbrechen (z.B. QS in Deutschland)
- **Worst Case Szenario**: Der vollständige Abfluss des eigenen Know-hows kann im schlimmsten Falle was zur Folge haben?

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Maßnahmen Technologietransfer

Auszug

APA: Technologietransfer nach China: Leitfaden für Unternehmer
Tel: 030 2028-1593

1. Falls **Joint-Venture-Zwang** besteht: Risiken besonders genau evaluieren

- Um bei **Ausschreibungen** mitzubieten – nur vertretbaren (worst case Szenario!) T-Transfer zulassen
- **CCC**: auf deutsche Werksinspektoren drängen, die im chinesischen Auftrag arbeiten

4. **Ingenieure sensibilisieren** – technische Fragen werden gerne offen diskutiert („Kollegen“)
5. **Nicht jeden Auftrag annehmen** – Vertrieb / Einkauf nicht sanktionieren, wenn man sich gegen „brisanten“ Auftrag entscheidet.

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

9. Maßnahmen im Bereich des Geheimschutzes/China

- **Zunächst ein paar Fragen:**

  Wieviel Euro steckt Ihr Unternehmen **jährlich in F&E?**

  Und in den Schutz dieser F&E-Ergebnisse?

  Ist **Corporate Security-Abteilung**, oder zumindest ein „erweiterter Werkschutz“ vorhanden?

  Werden Mitarbeiter, die im Ausland Verhandlungen führen oder als Expats eingesetzt werden, nicht nur unter interkulturellen Gesichtspunkten („nice-to-have“), **sondern auch unter Sicherheits- und Geheimschutzaspekten** („damned duty“) geschult?

IHK Pfalz Kompetenzzentrum China

Geheimschutz in der Wirtschaft

Maßnahmen im Bereich des Geheimschutzes

kleiner Auszug

- **Konkrete praktische Geheimschutzmaßnahmen – allgemein und speziell im China-Geschäft (kleiner Auszug)**

1. **Nicht nur Spitzentechnologie** ist für Industriespionage interessant! Auch Verfahrenswissen und Preispolitiken, etc. sind Ziel von Angriffen.
2. Spezielle **Vorbereitung** der ins China-Projekt involvierten Delegationsmitglieder
3. **Verhaltenskodex** aufstellen und vom Mitarbeiter unterschreiben lassen! Strafrechtliche Konsequenzen darstellen.
4. **Vertrauliches Firmenmaterial** auf Geschäftsreisen niemals im Hotelzimmer lassen, Einbruchsgefahr.
5. „**China-Laptop**“ mitnehmen – so wenig wie möglich Infos.

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Geheimschutz in der Wirtschaft

Maßnahmen im Bereich des Geheimschutzes

Im Haifischbecken schwimmen lernen

- **Konkrete praktische Geheimschutzmaßnahmen**

6. **Besondere Vorsicht auf Messen:** Laptop-Diebstahl. Müssen die innovativsten Maschinen ausgestellt werden?
7. Chefetage, F&E und Konferenzräume sollten durch qualifizierte Dienstleister **regelmäßig entwanzt** werden und die Fenster mit schallschluckenden Vorhängen versehen werden.
8. Räume für vertrauliche Gespräche immer erst kurzfristig festlegen und regelmäßig wechseln.
9. Nachrichten nur verschlüsselt per Fax senden; Aufpassen: Zwischenspeicher! Wenn möglich **VPN einrichten.**
10. **Chinesische Praktikanten**, Studenten, Diplomanden und Doktoranden grundsätzlich nicht in sensiblen Abteilungen!

IHK Pfalz Kompetenzzentrum China

Geheimschutz in der Wirtschaft

Maßnahmen im Bereich des Geheimschutzes

Im Haifischbecken schwimmen lernen

- **Konkrete praktische Geheimschutzmaßnahmen**

<u>Mitarbeiterbindungsprogramm</u> für China erarbeiten:

Personal: fast jeder Mitarbeiter ist auch „Unternehmer“

- Fortbildung & Aufstiegschancen: **Vision**
- Entlohung
- Chef als fürsorglicher Vater
- gesichtswahrendes Arbeitsklima (!)
- Familienfeste, Gründung eines gem. Sportvereins
- Mietzuschuss
- Individuelle Wünsche erfüllen (2. Kind...)

wichtig - hat aber Grenzen...

© Andreas Blume 2006

IHK Pfalz
Kompetenzzentrum China

Maßnahmen im Bereich des Geheimschutzes

Ergo:

Nicht warten, bis Spionagefall eingetreten ist!

Aktuelle Informationen bei **kompetenten Partnern einholen:**

→ **Landesämter für Verfassungsschutz** oder entsprechende Abteilungen der jeweiligen **Innenministerien**

→ **Verband für Sicherheit in der Wirtschaft**: www.vsw-service.com

→ **Weitere Infos: BfV** www.verfassungsschutz.de

→ www.sicherheitsforum-bw.de (**Schutzkonzept**)

IHK Pfalz
Kompetenzzentrum China

10. IP-Schutzmaßnahmen

Ein **ganzheitliches Technologieschutzkonzept** muss zusätzlich ein unternehmensspezifisches, individuelles **„Anti-Counterfeiting-Paket“** als präventives und reaktives Maßnahmen-Portfolio beinhalten.


Destroying pirated optical discs

Es existieren über **60 Einzelmaßnahmen**, die aus den Bereichen: **Recht, Technik, Betriebswirtschaft, Unternehmens-politik und Politik** kombiniert werden können, um Produktpiraten das Leben zu erschweren bzw. die negativen Konsequenzen für Unternehmen zu reduzieren.

Im Haifischbecken schwimmen lernen

IHK Pfalz

IP-Schutzmaßnahmen

Im Haifischbecken schwimmen lernen

- **Schritt #1: Problemanalyse: Größe & Art Problem:**

  Nachforschungen anstellen:

  - in Eigenregie: über Märkte und Messen gehen
  - Reporting der Vertriebsorganisation
  - Vertragshändler & Agenten
  - Kunden und Geschäftspartner (Unternehmen)
  - Detektive
  - Spez. Dienstleister und Internetkontrolleure

IHK Pfalz

IP-Schutzmaßnahmen

Im Haifischbecken schwimmen lernen

- **Schritt #2: Bewertung der unternehmens- und produktspezifischen Faktoren**

  Was will ich erreichen?

  → Nur: Schutz vor unberechtigter Produkthaftung und und Schadensersatz? Schutz innerhalb der EU?

  → Oder: Kampf gegen Reputationsverlust und Umsatzeinbußen?

  → Sogar direkte Auseinandersetzung mit Fälschern?

  Was darf es maximal kosten? Szenarien entwickeln zur Kosten-Nutzen-Abwägung

IHK Pfalz Kompetenzzentrum China

IP-Schutzmaßnahmen

Im Haifischbecken schwimmen lernen

- **Schritt #3: Kenntnis des chinesischen „IP-Regimes“**

- Welche Maßnahmen führen in China **leicht**, nur mit **erheblichem Aufwand** oder gar **nicht** zum Erfolg?
- Welche Präventivmaßnahmen sind sinnvoll?
- Welche Maßnahmen müssen kombiniert werden, damit sich Erfolg einstellt?
- Welche Partner brauche ich dafür?

- **Schritt #4: Wer wird Anti-Counterfeiting-Beauftragter?**

IHK Pfalz Kompetenzzentrum China

IP-Schutzmaßnahmen

Im Haifischbecken schwimmen lernen

- **Vorsicht: 4 typische Fehler & folgenschwere Fehleinschätzungen:**

1. Counterfeiting ist eine rein „rechtliche Angelegenheit“ → Rechtsabteilung
2. Den Kopf in den Sand stecken! „Kann sowieso nichts dagegen tun!“
3. „Ich bin nicht betroffen!“
4. „Anti-Counterfeiting können sich doch nur Großunternehmen leisten!“

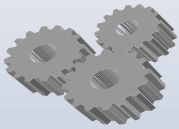
IHK Pfalz
Kompetenzzentrum China

IP-Schutzmaßnahmen

Basisschutz – „magisches Sechseck“

Vitales Know-how nur unter bestimmten Voraussetzungen transferieren

IP-Rechte sichern



Grenzbeschlagnahme in EU

Messebeschlagnahme in Europa/Deutschland

Produkte kennzeichnen

PR: Kunden aufklären/ Mitarbeiter sensibilisieren

Im Haifischbecken schwimmen lernen

IHK Pfalz
Kompetenzzentrum China

IP-Schutzmaßnahmen

Quelle: Suesse, Tesa Scribos

tesa scribos

Sicherheitskriterien

verdeckt
im Labor auswertbar
oder Kodierung, variable Daten

verdeckt
mit speziellem Hilfsmittel auswertbar

verdeckt
mit einfachem Hilfsmittel auswertbar

offen
mit bloßem Auge auswertbar

Opt. Verfahren
Chip RFID
Taggants
Magn. Verfahren

Magn. Verfahren
opt. Verfahren
Farbstoffe
Chipless RFID

Drucktechniken
Farbstoffe
Barcodes

Hologramme
Drucktechniken
Schichtsysteme

Ludwigshafen, 12. Februar 2004

IP-Schutzmaßnahmen

- **Grenzbeschlagnahmeantrag für EU stellen**
  - **Zentralstelle Gewerblicher Rechtsschutz ZGR**
  - ZGR mit bundesweiter u.europaweiter Zuständigkeit
  - Beschlagnahme 2004/2005: 8.500/7.200 Sendungen
  - **Alle erteilten Leistungsschutzrechte können geschützt werden**
  - Nähere Infos: **www.grenzbeschlagnahme.de**
    Leiter ZGR: Klaus Hoffmeister: Tel: 089 5995-2313

IP-Schutzmaßnahmen

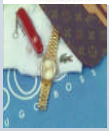
- **PR: Kunden aufklären/Mitarbeiter sensibilisieren**
  - **Aufklärungskampagnen** gegenüber Kunden hinsichtlich Schäden, Gefahren und Hintergründe von Counterfeiting
  - Sichtbare Sicherungskennzeichen **geg. Kunden kommunizieren**
  - **Kundenhotline/Webauftritt einrichten**
  - **Mitarbeiter speziell schulen** (Erkennung von Fälschungen). Anreize. Versicherungs-, straf- und personalrechtliche Konsequenzen erläutern.

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Literaturhinweis

- **Produktpiraterie in China**



Praxisbezogene Dissertation 1/2006

- Phänomen: IP-Verletzungen, Arbeitsweise der Täter
- Recht- und Rechtsdurchsetzung
- Schattensystem und „IP-Widerstände“

3 Teilstudien, zu beziehen unter:

www.chinapolitik.de

東

Im Haifischbecken schwimmen lernen

IHK Pfalz Kompetenzzentrum China

Vielen Dank für Ihre Aufmerksamkeit !

Denn: Hinter der großen Mauer

lauern Chancen - aber auch Gefahren!

Stellen Sie sich deshalb aktiv dem Drachen!

Dr. Andreas Blume M.A.
Leiter Kompetenzzentrum VR China
der IHK Pfalz
Tel: 0621 5904-1920
Fax: 0621 5904-1904
Mail: andreas.blume@pfalz.ihk24.de
www.pfalz.ihk24.de/china

Im Haifischbecken schwimmen lernen

Konkurrenzspionage – Risiken durch den Einsatz elektronischer Medien

Heiko Schmidt, Kriminaldirektor, Abteilungsleiter im Landeskriminalamt Thüringen

Meine Sehr verehrten Damen und Herren,

ich möchte Ihnen in meinem Power-Point-Vortrag einen praxisnahen Einblick in die vielfältigen Möglichkeiten geben, mit elektronischen Medien Konkurrenzspionage zu betreiben.
Im Rahmen einer Realdemonstration werde ich Ihnen vorführen, wie sich mit entsprechend simplen Methoden und der entsprechenden Software einen Hackerangriff auf ein Computernetzwerk vollzieht.

Konkurrenzspionage – Risiken durch den Einsatz elektronischer Medien

Vortrag aus Anlass des Gemeinsamen Symposiums
der IHK Erfurt, des LfV und des LKA Thüringens

❖

28. November 2006

❖

Kriminaldirektor Heiko Schmidt

Landeskriminalamt Thüringen / Abteilung 6

Disposition

Landeskriminalamt Thüringen

- **Einführung**
- **Gefährdungsszenarien**
- **Beispiele**
- **Präventionshinweise**

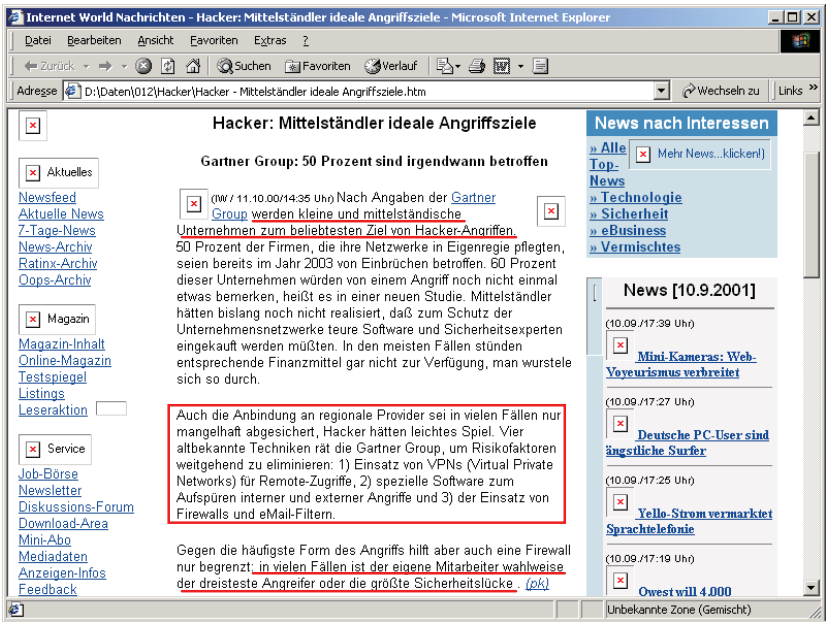
Europäisches Parlament

BERICHT über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)) vom 11. Juli 2001

Landeskriminalamt Thüringen

„Das Risiko- und Sicherheitsbewusstsein bei kleinen und mittleren Unternehmen ist bedauerlicherweise oft unzureichend, und die Gefahren der Wirtschaftsspionage und des Abhörens von Kommunikation werden oft nicht erkannt. Da auch bei europäischen Institutionen (...) das Sicherheitsbewusstsein nicht immer sehr ausgeprägt ist, besteht unmittelbarer Handlungsbedarf.“

Landeskriminalamt Thüringen / Abteilung 6



Dr. Udo Helmbrecht, Präsident BSI
(7. Datenschutzkongress, Berlin, 11.05.2006)

Landeskriminalamt Thüringen

…die IT-Sicherheitskompetenz ist in Deutschland nur unzureichend verbreitet. Obwohl Bürgerinnen und Bürger immer mehr von Informationstechnik abhängen – sei es am Arbeitsplatz, beim Zahlungsverkehr, in der Kommunikation oder im E-Commerce – räumen nur wenige sicherer Informations-technik in der Praxis den erforderlichen Stellenwert ein …

heise online - Telekom-Router zu offen file:///D:/Datenaustausch/81233.htm

news 18.11.2006 19:40

heise Netze
<< Vorige | Nächste >>

Telekom-Router zu offen

Der neue Telekom-Chef René Obermann sagt zwar, sein Konzern müsse "in vielen Bereichen schneller reagieren, freundlicher sein". Doch zu Hackern war die Telekom stellenweise schon vor seinem Amtsantritt zu freundlich: Der ADSL-WLAN-Router Speedport W 700V stellt in der ausgelieferten Firmware-Version 1.07 die Browser-Konfiguration auch über das Internet zur Verfügung. Zwischen einem Angreifer aus dem Internet und der vollen Kontrolle über den Router und das daran angeschlossene Netzwerk steht nur noch das Konfigurations-Passwort. Freundlicherweise zeigt der Router das Standard-Passwort auch noch auf der Eingangsseite an.

Der ADSL-WLAN-Router Speedport W 700V zeigt Einbrechern freundlicherweise das Default-Passwort an.

Dieser Fernkonfigurationszugang lässt sich in den Browserseiten des Routers nicht schließen. Ein konfigurierbarer Pakerfilter, mit dem sich der Port verriegeln ließe, fehlt dem Gerät. Nur ein Firmware-Update auf die Version 1.16 schließt die Lücke zuverlässig.

Der Speedport W 700V stammt vom Zulieferer Arcadyan, einem Joint-Venture zwischen der SMC-Mutter Accton Technology und Philips und gehört zu mehreren T-DSL-Paketangeboten der Telekom. Der Speedport W *701V* vom Zulieferer AVM ist von diesem Fehler nicht betroffen.

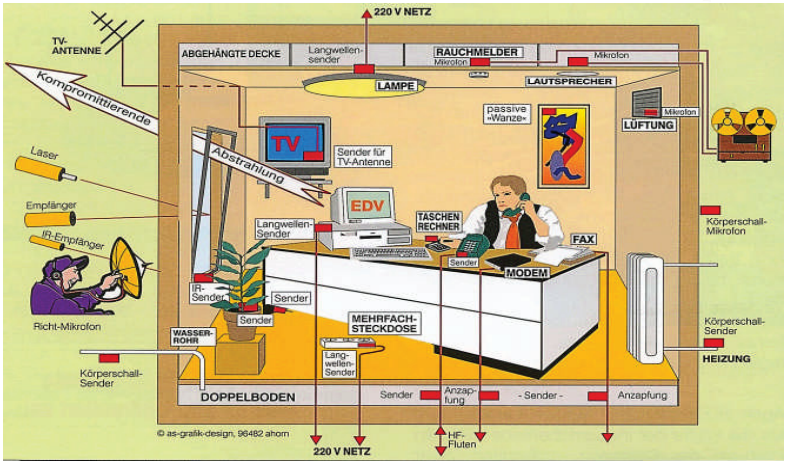
Polizeiliche Kriminalstatistik Thüringen (PKS)

Landeskriminalamt Thüringen

- Relevanter Tatbestand = § 202a StGB (Ausspähen von Daten)
- 2006 = 24 sog. PHISHING-Fälle mit einem Gesamtschaden von ca. 119.000 EUR
- Keine Strafanzeigen zu sonstigen Konkurrenzdelikten unter Einsatz von EDV

Gefährdungsszenarien Allgemein

Landeskriminalamt Thüringen



Gefährdungsszenarien - Einsatz von PC

Landeskriminalamt Thüringen

• Verlust der Vertraulichkeit (Spionageaspekt)	• Ausspähen von Daten • Verrat Betriebsgeheimnisse
• Verlust der Integrität (Sabotageaspekt)	• Datenveränderung • Sabotage: z. B. frustr. MA
• Verlust der Verfügbarkeit (Funktionsverlust)	• Diebstahl der Technik • Systemabsturz
• Verlust der Authentizität (Echheitsbeweis v. Daten)	• Digitale Unterschrift • E-Commerce

Keyghost

Landeskriminalamt Thüringen

Dr. Udo Helmbrecht, Präsident BSI
(7. Datenschutzkongress, Berlin, 11.05.2006)

Landeskriminalamt Thüringen

… Das Internet eröffnet der Wirtschafts- und Konkurrenzspionage neue Dimensionen. Die Methoden zum Ausspähen und Manipulieren von Daten und Diensten werden zunehmend professioneller. Neben klassischen Technologie- und Know-how-Diebstahl gewinnt die Erlangung von Wettbewerbsvorteilen an Bedeutung, etwa durch das Ausspionieren von Ausschreibungen, Verträgen und Preisinformationen. Das Ausspähen von Unternehmensnetzen mit dem Ziel der unbefugten Kenntnisnahme von Unternehmensdaten nimmt zu …

Gefährdungsszenarien - Internet

- offene Datenübertragung
  - Daten können: mitgelesen, verändert, wiedereingespielt, mißbräuchlich verwendet oder zerstört werden (z. B. Sniffer)
- Konzeptions- Konfigurations- und Programierungsfehler
  - IP-Spoofing, Source Routing, ICMP

Straftaten im Internet:

Pornografie, Prostitution, Beleidigungsdelikte, Gewaltverherrlichung, politischer Extremismus, Betrug, Geldwäsche, Erpressungsdelikte, Sabotage, Spionage, unlauterer Wettbewerb, Lotterie- und Glücksspiel, BtM-Delikte, Urheberrechtsverstöße, Domain-Name-Grabbing, Körperverletzungs- und Tötungsdelikte

Dr. Udo Helmbrecht, Präsident BSI
(7. Datenschutzkongress, Berlin, 11.05.2006)

... Eine zunehmende Bedrohung geht von Schad- und Spionageprogrammen aus. Dabei begünstigt die starke Verbreitung von Standardsoftware den Wirkungsgrad dieser Schädlinge. Durch die Dominanz einzelner Produkte am Markt sind die in diesem Produkt vorhandenen Schwachstellen besonders weit verbreitet. Dies führt bei Ausnutzung zu hohen Schäden. Angreifer nutzen dies gezielt ...

Hauptquelle für die Verteilung von Computerviren sind die arglosen Nutzer von Privat- und Unternehmensrechnern!

Präventionsstrategien - Einsatz von PC

(Büroraum - Aufstellungsort PC)

- bei Abwesenheit Türen u. Fenster schließen
- mechanische. u. technische Sicherungsmaßnahmen nutzen
- Zugangsregelung Raum
- Beaufsichtigung Fremdpersonal

(Systembezogene Sicherheit)

- Paßwortschutz/Bildschirmsperre
- Virensuchprogramme/Verhaltensregeln
- Nutzung progr. Sicherungsfunktionen
- Verschluß von Laufwerken
- Datensicherung am PC
- sichere Aufbewahrung Datenträger
- Sicherungskopien aller Software
- sporadische Prüfung Wiederherstellbarkeit von Daten u. Dateien
- Erstellung PC-Notfalldiskette
- Sichern des CMOS-RAM
- Schutz gg. kompromit. Abstrahlung
- Überspannungsschutz/Stromversorgung

Präventionsstrategien - Einsatz Internet

- Verschlüsselung
- Einsatz von Zugriffskontrollverfahren
- umfassendes Aufklären u. Sensibilisieren der User
- Schutzkonzepte/Richtlinien
- personelle u. organisatorische Regelungen für den Internetzugang (wer darf wann, was)
- Absicherung der zugelassenen Dienste durch Firewallsysteme
- Notfall- u. Maßnahmepläne für erkannte Hackerangriffe

Herzlichen Dank für Ihre Aufmerksamkeit!

Das Landeskriminalamt Thüringen erreichen Sie unter:

0361/341-0

oder

www.polizei.thueringen.de/lka/

bzw.

lka@polizei.thueringen.de

Autoren

Martin Kaufmann
Sachbereichsleiter Presse- und Öffentlichkeitsarbeit Thüringer Landesamt für Verfassungsschutz

Dr. Andreas Blume
Leiter Kompetenzzentrum VR China der IHK Pfalz, Ludwigshafen
zwischenzeitlich
Degussa GmbH
Creavis Technologies & Innovation Science to Business Center
S-IPM-CI
Paul-Baumann-Straße 1
45764 Marl
T +49 2365 49-7169 und -7329
F +49 2365 49-807169 und -6440
E-mail: andreas.blume@degussa.com

Heiko Schmidt
Kriminaldirektor, Abteilungsleiter im Landeskriminalamt Thüringen

Herausgeber

Thüringer Landesamt

für Verfassungsschutz
Öffentlichkeitsarbeit und
Berichtswesen

Haarbergstraße 61, 99097 Erfurt
Tel. 0361/4406-0
Fax: 03614406-251
http:// www.verfassungsschutz.thueringen.de
e-mail: kontakt@lfv.thueringen.de

Landeskriminalamt Thüringen
Pressestelle

Am Schwemmbach 69, 99099 Erfurt
Tel. 0361/341-1107
Fax: 0361/341-1009
http:// polizei.thueringen.de
e-mail: pressestelle.lka@polizei.thueringen.de

Erfurt 2007